日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　３月１９日
出願番号 Application Number: [ST. 10/C]:	特願２００３－０７５８６５ [ＪＰ２００３－０７５８６５]
出願人 Applicant(s):	株式会社日立製作所

U.S. Appln. Filed 3-18-04
Inventor: T. Yasue et al
Mathingly Stanger & Malur
Docket HAS-101

２００４年　３月　４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０１６８６６

【書類名】　特許願
【整理番号】　P0637JP
【提出日】　平成15年 3月19日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/46
【発明者】
　【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
　【氏名】　安江　利一
【発明者】
　【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
　【氏名】　綿貫　達哉
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社日立製作所
【代理人】
　【識別番号】　100107010
　【弁理士】
　【氏名又は名称】　橋爪　健
【手数料の表示】
　【予納台帳番号】　054885
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0104115
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワーク認証装置及びネットワーク認証システム

【特許請求の範囲】

【請求項１】

ユーザ認証を行い、ネットワークを介してユーザ端末と情報サーバとの間でパケットを送受信するネットワークシステムにおけるネットワーク認証装置であって、

ユーザ端末及び情報サーバに対してパケットを送受信するネットワークインタフェース部と、

受信したパケットを中継すべき前記ネットワークインタフェース部を示す情報が登録されるアドレステーブルと、

入力されたパケットを、該パケットの宛先アドレスに基づき、前記アドレステーブルが示す前記ネットワークインタフェース部を介して中継するパケット中継部と、

パケットの中継又は廃棄を示す情報が登録されており、認証されたユーザ端末からのパケットを中継するように情報が更新されるフィルタリングテーブルを有し、前記ネットワークインタフェース部を介して受信したパケットの宛先アドレスに対応する、送信元ＭＡＣアドレスと送信元ＩＰｖ６アドレスとの両方の情報に基づき、前記フィルタリングテーブルを参照して条件を判断し、該受信したパケットを前記パケット中継部へ中継する又は廃棄するフィルタリング処理部と、

を備えたネットワーク認証装置。

【請求項２】

送信元ＩＰｖ６アドレスとして、送信元ＩＰｖ６アドレスのインタフェース識別子を用いる請求項１に記載のネットワーク認証装置。

【請求項３】

ユーザ認証によりアクセスが許可されたユーザ端末からのパケットを中継させるための状態変更指示を受信し、該状態変更指示に従い前記フィルタリングテーブルを変更するフィルタ変更指示処理部をさらに備え、

前記フィルタリング処理部は、変更された前記フィルタリングテーブルに基づ

いて、アクセスが許可されたユーザ端末からのパケットを中継する請求項１に記載のネットワーク認証装置。

【請求項４】

前記フィルタリング処理部は、受信したパケットから宛先アドレス、送信元ＭＡＣアドレス及び送信元ＩＰｖ６アドレスの複数の情報を抽出し、前記フィルタリングテーブルの対応する情報と比較し、全ての情報で中継と判断した場合に該パケットを前記パケット中継部へ中継する請求項１に記載のネットワーク認証装置。

【請求項５】

前記フィルタリング処理部は、

宛先ＭＡＣアドレス及び送信元ＭＡＣアドレスに対応して受信パケットの中継又は廃棄を示す情報が登録されたＭＡＣアドレスフィルタリングテーブルと、

宛先ＩＰｖ６アドレス及び送信元ＩＰｖ６アドレスに対応して受信パケットの中継又は廃棄を示す情報が登録されたＩＰｖ６アドレスフィルタリングテーブルと、

前記ＭＡＣアドレスフィルタリングテーブルを参照して、受信パケットを中継又は廃棄するＭＡＣアドレス処理部と、

前記ＩＰｖ６アドレスフィルタリングテーブルを参照して、受信パケットを中継又は廃棄するＩＰｖ６アドレス処理部と

を有し、

前記ＭＡＣアドレス処理部と前記ＩＰｖ６アドレス処理部との両方で中継すると判断された受信パケットのみ、前記パケット中継部へ中継する請求項１に記載のネットワーク認証装置。

【請求項６】

ユーザ識別子、パスワード、ＩＰｖ６アドレスのインタフェース識別子及びＭＡＣアドレスが記憶され、ユーザ端末からの要求に従いユーザ認証を行う認証処理部をさらに備えた請求項１に記載のネットワーク認証装置。

【請求項７】

前記認証処理部は、

ユーザ端末からのユーザ認証要求を受け付け、ユーザ識別子、パスワード、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータをユーザ端末から受け取る認証受付処理部と、

ユーザ端末から受け取った認証パラメータと予め記憶された認証用データとに基づきユーザ及びその端末を認証し、認証した場合に、前記フィルタ変更指示処理部に認証したユーザ端末からのパケットを中継させるための状態変更指示を送信する認証部

を有する請求項６に記載のネットワーク認証装置。

【請求項８】

通信相手毎に鍵交換処理を行って通信パスを確立し、通信相手毎に鍵交換処理により作成した鍵、及び、通信相手の認証を行うための予め定められた鍵若しくは認証情報を格納するＩＰセキュリティ制御部と、

前記ＩＰセキュリティ制御部により作成された鍵を用いたパケットの暗号化及び復号化機能、及び、パケット改ざんチェック機能、及び、前記ＩＰセキュリティ制御部に記憶されている予め定められた鍵若しくは認証情報に基づく通信相手の認証機能とを有するＩＰセキュリティ処理部と

をさらに備え、

前記ＩＰセキュリティ処理部は、通信相手を認証した場合にパケットを前記フィルタリング処理部へ送信し、一方、認証されなかった場合にパケットを廃棄する請求項１に記載のネットワーク認証装置。

【請求項９】

請求項１に記載のネットワーク認証装置と、

ネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、

を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システム。

【請求項１０】

前記ネットワーク認証装置と前記ユーザ端末は、広域イーサネット（登録商標）網で接続されていることを特徴とする請求項９に記載のネットワーク認証システム。

【請求項１１】

請求項１に記載のネットワーク認証装置と、

パケットを中継するためのルータと、

前記ルータ及びネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ルータに接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、

を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システム。

【請求項１２】

請求項８に記載のネットワーク認証装置と、

前記ネットワーク認証装置との間で鍵交換処理を行ってＩＰセキュリティ通信

パスを生成し、鍵交換処理により作成した鍵を用いてパケットを暗号化及び復号化し、該ＩＰセキュリティ通信パスを介して前記ネットワーク認証装置と通信するユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、

を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子、前記ユーザ端末と前記認証サーバに格納されている予め定められた同一の鍵のいずれか又は複数を含む認証パラメータを受け取り、該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク認証装置及びネットワーク認証システムに係り、特に、アクセスが許可された端末からのパケットを中継するネットワーク認証装置、及び、ネットワーク認証システムに関する。

【０００２】

【従来の技術】

各種情報機器及び通信機器の発達によりネットワークの利用が増え、それに伴い、ネットワークが保持する情報に対する信用を確保するために、ネットワークの利用を制限する情報セキュリティ技術の必要性が認識されている。例えば、外部からの不正な利用者や、利用を許可されていない内部の者であっても、ネットワークに接続されているサーバにアクセスが可能である。これらの不正なアクセスを防止する手段として、ユーザＩＤとパスワードを使ったユーザ認証やルータ

等の通信機器によるパケットフィルタリングが知られている（例えば、特許文献１参照）。

【０００３】

パケットフィルタリングには、同一サブネット内でパケット（フレーム）を中継するＬ２スイッチ（例えば、ＬＡＮスイッチ）によるＭＡＣ（Media Access Control）フィルタリングと、異なるサブネット間でパケットをルーティングするルータによるＩＰフィルタリングが知られている。また、Ｌ２(Layer 2)スイッチとルータを切り替えるマルチレイヤスイッチが提案されている。

【０００４】

図２８は、マルチレイヤスイッチによるフィルタリング処理の概略図である。マルチレイヤスイッチは、例えば、Ｌ２スイッチ機能１０と、ルータ機能２０と、レイヤー判断部３０とを備える。Ｌ２スイッチ機能１０のＭＡＣアドレス処理部１１は、ＭＡＣアドレスフィルタリングテーブル１２を参照し、ＭＡＣアドレス（物理アドレス）に基づきパケットをフィルタリングする。また、ルータ機能２０のＩＰアドレス処理部２１は、ＩＰアドレスフィルタリングテーブル２２を参照し、ＩＰアドレスに基づきパケットをフィルタリングする。ルータ機能２０は、さらにＭＡＣヘッダ除去やホップ数の変更など適宜のルーティング処理を行う場合もある。レイヤー判断部３０は、例えば、受け取ったパケットの宛先ＩＰサブネットと入力ポートのサブネットが同一である、又は、宛先ポートと入力ポートが同一ＶＬＡＮ（Virtual LAN）である等の条件に基づき、Ｌ２スイッチ機能１０又はルータ機能２０のいずれかにパケットを中継する。図２８に示すように、マルチレイヤスイッチは、レイヤー判断部３０の判断結果に基づき、ＭＡＣアドレス又はＩＰアドレスのいずれか一方のみによりフィルタリングする。したがって、通常のＬ２スイッチ及びルータと比較してセキュリティ強度に大きな違いは生じない。

【０００５】

また、広域イーサネット（登録商標）サービスが始まり、これを用いて企業と家庭（ＳＯＨＯ、Small Office Home office）を結ぶ広域ＶＰＮ（Virtual Private Network）の構築が可能となっている。しかし、広域イーサネット（登録商

標）は、簡単に使える反面、セキュリティ強度が低いという課題がある。

【０００６】

さらに、ＡＤＳＬ(Asymmetric Digital Subscriber Line)、ケーブルテレビ等に代表される常時接続ブロードバンドの普及により、リモートオフィス化の要求が増大している。企業の本社と家庭（ＳＯＨＯ）又は支店を結ぶ企業イントラネットを、インターネットとＩＰｓｅｃ（IP security protocol、ＩＰセキュリティ）を組み合わせたインターネットＶＰＮで安く構築しようというものである。企業イントラネットといっても各事業所には独自のポリシがあり、同じ企業の社員であっても他の事業所からは特定のユーザからのアクセスのみ許可するのが一般的である。そのため、独自のポリシに基づくセキュリティ対策、セキュリティシステムが必要となる。しかし、インターネットＶＰＮでは、ルータを介したネットワーク間でＶＰＮを構成するため、ＭＡＣアドレスによる認証及びフィルタリングはできず、ＩＰｖ４アドレスでのフィルタリング等が行われている。

【特許文献１】

特開２００２－８４３０６号公報

【０００７】

【発明が解決しようとする課題】

従来のＩＰｖ４（Internet Protocol version 4）アドレスを用いたインターネットの場合、ユーザ端末が移動すると、移動先でＤＨＣＰ(Dynamic Host Configuration Protocol)サーバから新たにＩＰアドレスの配布を受け、その度にＩＰアドレスが変化する。そのため、ＩＰアドレスをユーザ認証やフィルタのパラメータとして使用することができない場合があった。すなわち、従来のＩＰｖ４アドレスによるユーザ認証及びフィルタリングを行うシステムでは、モビリティとセキュリティの両方を確保することが困難であった。また、同一ＩＰｖ４アドレスに成りすました侵入者に対するセキュリティが低いという課題がある。

【０００８】

また、例えば、インターネットＶＰＮ等のルータを介するネットワークでは、ユーザ端末のＭＡＣアドレスがルータのアドレスに付け替えられるため、装置固有の情報を用いたユーザ認証、及び、パケットフィルタリングができない課題が

ある。

【０００９】

本発明は、以上の点に鑑み、アクセスが許可されていない端末からのアクセス、及び、なりすましによる侵入者からのアクセスを拒否する高セキュリティなネットワークシステムを構築することを目的とする。また、本発明は、ＩＰｖ６アドレスのインタフェースＩＤ部分を活用してセキュリティ強度の高いユーザ認証及びパケットフィルタリングを行うことを目的とする。特に、ルータを介して通信を行うネットワークシステムにおいて、従来のＩＰｖ４アドレスによるフィルタリングよりも強度の高いセキュリティシステムを提供することを目的する。また、本発明は、ユーザ端末の移動に対しても高いセキュリティ強度を有するモビリティの優れたシステムを提供することも目的のひとつである。

【００１０】

さらに、本発明は、Ｌ２スイッチにＩＰフィルタリング機能を持たせ、ＭＡＣアドレス及びＩＰアドレス等をパラメータとした多段フィルタリングを行い、セキュリティ強度を高くすることを目的とする。本発明は、ユーザＩＤ及びパスワードに加えてＩＰｖ６（Internet Protocol version 6）アドレスのインタフェースＩＤ及びＩＫＥ(Internet Key Exchange)のユーザ認証機能を併用することによりユーザ認証の確度を高めることを目的とする。また、本発明は、広域イーサネット（登録商標）、構内データセンタ、インターネットＶＰＮ等のネットワークにおける高セキュリティなネットワークシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

本発明の第１の解決手段によると、

ユーザ認証を行い、ネットワークを介してユーザ端末と情報サーバ間でパケットを送受信するネットワークシステムにおけるネットワーク認証装置であって、

ユーザ端末及び情報サーバに対してパケットを送受信するネットワークインタフェース部と、

受信したパケットを中継すべき前記ネットワークインタフェース部を示す情報

が登録されるアドレステーブルと、

入力されたパケットを、該パケットの宛先アドレスに基づき、前記アドレステーブルが示すネットワークインタフェース部を介して中継するパケット中継部と、

パケットの中継又は廃棄を示す情報が登録されており、認証されたユーザ端末からのパケットを中継するように情報が更新されるフィルタリングテーブルを有し、前記ネットワークインタフェース部を介して受信したパケットの宛先アドレスに対応する、送信元ＭＡＣアドレスと送信元ＩＰｖ６アドレスとの両方の情報に基づき、前記フィルタリングテーブルを参照して条件を判断し、該受信したパケットを前記パケット中継部へ中継する又は廃棄するフィルタリング処理部と、を備えたネットワーク認証装置が提供される。

【００１２】

本発明の第２の解決手段によると、

上記ネットワーク認証装置と、

ネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、

を備え、

前記認証サーバは、前記ユーザ端末から、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システムが提供される。

【００１３】

本発明の第３の解決手段によると、

上記ネットワーク認証装置と、

パケットをルーティングするためのルータと、

前記ルータ及びネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ルータに接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、

を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システムが提供される。

【００１４】

本発明の第４の解決手段によると、

通信相手毎に鍵交換処理を行って通信パスを確立し、通信相手毎に鍵交換処理により作成した鍵、及び、通信相手の認証を行うための予め定められた鍵若しくは認証情報を格納するＩＰセキュリティ制御部、及び、

前記ＩＰセキュリティ制御部により作成された鍵を用いたパケットの暗号化及び復号化機能、及び、パケット改ざんチェック機能、及び、前記ＩＰセキュリティ制御部に記憶されている予め定められた鍵若しくは認証情報に基づく通信相手の認証機能とを有し、通信相手を認証した場合にパケットを前記フィルタリング処理部へ送信し、一方、認証されなかった場合にパケットを廃棄するＩＰセキュリティ処理部をさらに備えた前記ネットワーク認証装置と、

前記ネットワーク認証装置との間で鍵交換処理を行ってＩＰセキュリティ通信パスを生成し、鍵交換処理により作成した鍵を用いてパケットを暗号化及び復号化し、該ＩＰセキュリティ通信パスを介して前記ネットワーク認証装置と通信するユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、

を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、ＭＡＣアドレス、ＩＰｖ６アドレス又は該アドレスのインタフェース識別子、前記ユーザ端末と前記認証サーバに格納されている予め定められた同一の鍵のいずれか又は複数を含む認証パラメータを受け取り、該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システムが提供される。

【００１５】

【発明の実施の形態】

１．ネットワーク認証ノード

図１は、ネットワーク認証システムの基本構成図である。ネットワーク認証システムは、ＩＰｖ６(Internet Protocol version 6)で通信可能な認証ノード（ネットワークノード）１００、認証サーバ２００、情報サーバ３００、情報端末（ユーザ端末）４００を備える。例えば、情報端末４００は、認証ノード１００と情報コンセント５０を介して接続される。

【００１６】

認証ノード１００は、情報端末４００から送られてきたパケットが、認証サーバ２００で認証を受けた情報端末４００からのパケットか逐一チェックし、パケットを中継又は廃棄する。例えば、ユーザ認証を受けていない情報端末４００から情報サーバ３００に送られたパケットは、認証ノード１００で廃棄される。認証ノード１００の詳細な構成及び処理は後述する。認証サーバ２００は、情報端末４００からの要求に従ってユーザ認証を行う。認証サーバ２００は、ユーザ認証が完了すると認証結果を認証ノード１００に通知し、認証を受けた情報端末４００からのパケットを中継させる。

【００１７】

図２は、ＩＰｖ６認証ノード１００の構成図である。認証ノード１００は、例えば、パケット中継部１１０、ネットワークインタフェース部ａ１２１～ｅ１２５、フィルタリング処理部１３１～１３５、フィルタ変更指示処理部１４０、ＩＰｖ６処理部１５０、アドレステーブル１６０を備える。なお、ネットワーク認証システムは、適宜の数のネットワークインタフェース部及びフィルタリング処理部を備えることができる。

【００１８】

ネットワークインタフェース部ａ１２１～ｅ１２５は、それぞれ異なる端末、サーバ又はネットワークに接続されており、パケットの送受信を行う。パケット中継部１１０は、パケットを受け取るとパケットの宛先に基づきアドレステーブル１６０を参照し、アドレステーブル１６０が示すネットワークインタフェース部ａ１２１～ｅ１２５を介してパケットを送信する。

【００１９】

図３は、フィルタリング処理部１３１～１３５の構成図である。フィルタリング処理部１３１～１３５は、それぞれパケット処理部５１０とフィルタリングテーブル５２０を備える。パケット処理部５１０は、ネットワークインタフェース部ａ１２１～ｅ１２５を介してパケットを受け取り、フィルタリングテーブル５２０の情報に基づいて、パケットの「中継」又は「廃棄」を判断する。パケット処理部５１０は、「中継」と判断した場合、受け取ったパケットをパケット中継部１１０へ送り、一方、「廃棄」と判断した場合、当該パケットを廃棄する。

【００２０】

フィルタリングテーブル５２０には、パケットの中継又は廃棄を判断するための情報が格納されている。例えば、宛先アドレス、送信元のＭＡＣアドレス、及び／又は、ＩＰｖ６アドレス、及び／又は、ＩＰｖ６アドレスのインタフェースＩＤ（以下、ＩＰｖ６インタフェースＩＤを記す）、パケットの中継／廃棄を示す情報が関連して格納されている。フィルタリングテーブル５２０は、フィルタ変更指示処理部１４０と接続されており、フィルタ変更指示処理部１４０により、テーブルの内容が変更される。例えば、初期状態では認証サーバ２００宛て以

外のパケットは廃棄するようにテーブルを構成し、認証サーバ２００により認証された端末からのパケットを中継するように、テーブルの内容を適宜変更する。

【００２１】

フィルタ変更指示処理部１４０は、認証サーバ２００と通信し、認証サーバ２００からフィルタリングテーブル５２０の状態変更指示を受信する。状態変更指示は、例えば、対象とするエントリの内容と、追加／削除の指示を含む。フィルタ変更指示処理部１４０は、状態変更指示を受信すると、フィルタリングテーブル５２０にその指示を反映させる。

【００２２】

ＩＰｖ６処理部１５０は、ルータ通知プロトコルを用いてユーザ端末４００にネットワークＩＤを通知する。ＩＰｖ６処理部１５０は、ルータ通知プロトコルを定期的に配信するが、
ユーザ端末４００からルータ要請プロトコルを受け取った場合にも同じようにネットワークＩＤを通知する。

【００２３】

なお、本実施の形態における認証ノード１００は、例えば、Ｌ２で動作するスイッチであり、ルータのようにホップ数の変更等のルーティング処理を行わない。Ｌ２で動作するスイッチにＭＡＣアドレス及びＩＰｖ６アドレスに基づくフィルタリング機能を持たせることにより、シンプルな構成で、セキュリティ強度が高い認証ノードを提供することができる。

【００２４】

図４は、認証サーバ２００の構成図である。認証サーバ２００は、認証受付処理部２１０と、実際にユーザ認証を行う認証部２２０を有する。認証受付処理部２１０は、情報端末４００からのユーザ認証要求を受け付ける処理部であり、ｗｅｂ認証ではポータルサイトに相当する。認証部２２０には、例えば、ユーザＩＤ（ユーザ識別子）、パスワード、ＩＰｖ６インタフェースＩＤ、ＭＡＣアドレスが関連付けられたテーブルが事前に認証用データとして格納されている。ユーザＩＤ、パスワードに加えてＩＰｖ６インタフェースＩＤを用いることでユーザＩＤ及びパスワードの不正使用によるアクセスを防止することが可能となる。さ

らに、認証部２２０には、ＩＫＥにおける通信相手の認証を行うための適宜の認証用データ（例えば、通信相手と同一の予め定められた鍵であるｐｒｅ－ｓｈａｒｅｄ　ｋｅｙ）が格納されていてもよい。

【００２５】

また、認証部２２０は、一般的に使われているＲＡＤＩＵＳ(Remote Authentication Dial In User Service)やＬＤＡＰ(Lightweight Directory Access Protocol)等の認証サーバを併用することもできる。さらに、認証サーバ２００は、外部装置として扱うだけでなく認証ノード１００に内蔵させることもできる。

【００２６】

情報サーバ３００は、情報端末４００に対して提供する情報を格納するサーバである。例えば、ファイルサーバや共有ファイルを有する情報端末等であり、情報端末４００からの要求に応じてデータを提供する。また、情報サーバ３００は、情報端末４００からの要求に応じた演算処理を行う演算装置であってもよい。

【００２７】

情報端末４００は、ＩＰｖ６で通信可能な端末である。例えば、Ｗｉｎｄｏｗｓ（登録商標）　ＸＰをＯＳとするパソコンを用いる事ができる。情報端末４００は、情報コンセント５０を介して認証サーバ２００によりユーザ認証を受け、ネットワーク内部の情報サーバ３００にアクセスする。

【００２８】

（変形例）

図５は、認証処理部を内蔵した認証ノードの構成図である。図５は、図１の認証サーバ２００の機能を内蔵した認証ノード２１００である。認証ノード２１００は、例えば、パケット中継部１１０、ネットワークインタフェース部ａ１２１～ｅ１２５、フィルタリング処理部１３１～１３５、フィルタ変更指示処理部１４０、アドレステーブル１６０、認証処理部２５０を備える。また、認証ノード２１００は、ＩＰｖ６処理部１５０をさらに備えてもよい。

【００２９】

図６は、認証処理部２５０の構成図である。認証処理部２５０は認証受付処理部２６０と認証部２７０を有する。なお、認証処理部２５０は、認証受付処理部

２５０だけを内蔵することもできる。認証受付処理部２６０及び認証部２７０の詳細は、図４に示す認証サーバの認証受付処理部２１０及び認証部２２０と同様である。認証処理部２５０は、パケット中継部１１０から認証要求パケットを受け取り、認証を行う。認証後、認証処理部２５０は、フィルタ変更指示処理部１４０にフィルタリングテーブル５２０の状態変更指示を送る。認証サーバ２００の機能を認証ノード２１００に内蔵することにより、認証前のパケットを構内に中継されることがなくなり、セキュリティ強度が上がる。

【００３０】

次に、ＩＰｖ６アドレスについて説明する。

図７は、ＩＰｖ６アドレスのアドレスフォーマットである。ＩＰｖ６アドレスは、上位６４ビットのネットワークＩＤと下位６４ビットのインタフェースＩＤで構成される。ネットワークＩＤは、ネットワーク上の通信機器によりルータ通知プロトコルを用いて、情報端末４００に通知される。インタフェースＩＤは、メーカＩＤと個別ＩＤを含む装置固有のＩＤである。従って、インタフェースＩＤは、接続先ネットワークが変わっても不変のＩＤである。なお、インタフェースＩＤ中の「ＦＦＦＥ」は、４８ビットのＭＡＣ（Media Access Control）アドレスから６４ビットのインタフェースＩＤを作成する場合に、メーカＩＤと個別ＩＤの間に挿入されるものである。

【００３１】

ネットワークに接続した情報端末４００は、ルータ要請プロトコル(Router Solicitation)を使って認証ノード１００（又はネットワーク内に存在するルータ）からネットワークＩＤを取得する。認証ノード１００は、情報端末４００からのルータ要請コマンドに従い、又は定期的に、ルータ通知プロトコル(Router Advertisement)を使って情報端末４００にネットワークＩＤを知らせる。ネットワークＩＤを取得した情報端末４００は、ネットワークＩＤと自身のインタフェースＩＤからＩＰｖ６アドレスを自動生成する。

【００３２】

図８は、フィルタリングテーブル５２０の構成例（１）を示す図である。フィルタリングテーブル５２０は、パケットの中継又は廃棄の判断のための情報を格

納しており、各エントリは、宛先アドレス条件フィールド６１０、送信元アドレス条件フィールド６２０、中継／廃棄フラグフィールド６３０を含む。宛先アドレス条件フィールド６１０には、宛先ＭＡＣアドレス又は「任意」を意味する情報が登録されている。なお、宛先アドレスとして、ＩＰｖ６アドレス等の適宜のアドレスを用いてもよい。送信元アドレス条件フィールド６２０は、送信元ＭＡＣアドレスフィールド６２１及び送信元ＩＰｖ６アドレスフィールド６２２を含み、それぞれＭＡＣアドレス、ＩＰｖ６アドレス又は「任意」を意味する情報が登録される。なお、本実施の形態においてアドレスの表記は、１６進数を用い、０は圧縮表記している。

【００３３】

中継／廃棄フラグフィールド６３０には、パケットの宛先アドレスと送信元アドレスがそれぞれ宛先アドレス条件と送信元アドレス条件に一致した受信パケットを中継すべきか又は廃棄すべきかを示す情報が登録されている。複数のエントリの情報と一致するパケットがあった場合は、テーブルの先頭に近いエントリがそのパケットに適用される。また、一致するエントリが一つもないパケットは、パケット処理部５１０によりパケット中継部１１０に送られる。

【００３４】

パケット処理部５１０によるフィルタリングは、ＭＡＣアドレスによるフィルタリング（ＭＡＣフィルタリング）と、ＩＰｖ６アドレスによるフィルタリング（ＩＰｖ６フィルタリング）を別個に行う独立フィルタリング方式とすることができる。パケット処理部５１０は、ＭＡＣフィルタリングする場合は、宛先ＭＡＣアドレスフィールド６１０及び送信元ＭＡＣアドレスフィールド６２１のＡＮＤ条件により、中継／廃棄フラグフィールド６３０の情報に従い「中継」又は「廃棄」を判断する。一方、パケット処理部５１０は、ＩＰｖ６フィルタリングする場合は、宛先ＭＡＣアドレスフィールド６１０及び送信元ＩＰｖ６アドレスフィールド６２２のＡＮＤ条件により、中継／廃棄フラグフィールド６３０の情報に従い「中継」又は「廃棄」を判断する。なお、送信元アドレス条件フィールド６２０にＭＡＣアドレスのみが登録されたＭＡＣアドレスフィルタリングテーブルと、ＩＰｖ６アドレスのみが登録されたＩＰｖ６アドレスフィルタリングテー

ブルが別々に格納されていてもよい。

【００３５】

また、パケット処理部５１０によるフィルタリングは、ＭＡＣアドレスとＩＰｖ６アドレスにより同時にフィルタリングする一括フィルタリング方式とすることもできる。パケット処理部５１０は、宛先ＭＡＣアドレスフィールド６１０、及び、送信元ＭＡＣアドレスフィールド６２１、及び、送信元ＩＰｖ６アドレスフィールド６２２のＡＮＤ条件により、中継／廃棄フラグフィールド６３０の情報に従い「中継」又は「廃棄」を判断することができる。

【００３６】

図９は、フィルタリングテーブル５２０の構成例（２）を示す図である。フィルタリングテーブル５２０の各エントリは、宛先アドレス条件フィールド６１０、送信元アドレス条件フィールド６２０、中継／廃棄フラグフィールド６３０を含む。送信元アドレス条件フィールド６２０は、送信元ＭＡＣアドレスフィールド６２１及び送信元ＩＰｖ６インタフェースＩＤフィールド６２３を含み、それぞれＭＡＣアドレス、ＩＰｖ６インタフェースＩＤ又は「任意」を意味する情報が登録されている。宛先アドレス条件フィールド６１０、中継／廃棄フラグフィールド６３０は上述と同様であるので説明を省略する。

【００３７】

図１０は、アドレステーブル１６０の構成例（１）を示す図である。アドレステーブル１６０の各エントリは、アドレスフィールド１６１、ネットワークインタフェース部フィールド１６２を含む。例えば、アドレスフィールド１６１にはＭＡＣアドレスが、インタフェース部フィールド１６２にはネットワークインタフェース部の識別子がそれぞれ格納される。アドレステーブル１６０の各エントリは、例えば、パケットを中継する際に、パケットの宛先アドレスに対応するネットワークインタフェース部からパケットを送信することを示している。また、アドレスフィールド１６１には、ＩＰアドレス等、適宜のアドレスを登録することもできる。

【００３８】

また、ルータ要請コマンドのパケットはＩＰｖ６処理部１５０へ中継するよう

にアドレステーブル１６０を構成する。例えば、アドレスフィールド１６１を自身のＭＡＣアドレス(22:22:00:FF:FF:FF)、ネットワークインタフェース部フィールドを「ｘ」としたエントリを登録する。パケット中継部１１０は、ネットワークインタフェース部として「ｘ」を取得した場合、当該パケットをＩＰｖ６処理部１５０へ中継する。さらに、宛先アドレスがブロードキャストアドレスであるパケットも、同様にしてＩＰｖ６処理部１５０へ中継させる。ＩＰｖ６処理部１５０は、パケットがルータ要請コマンドでない場合、適宜パケットを処理する。

【００３９】

なお、パケット中継部１１０が、受け取ったパケットがルータ要請コマンドであるか判断し、ルータ要請コマンドであればパケットをＩＰｖ６処理部１５０へ中継するようにしてもよい。ルータ要請コマンドでない場合、パケット中継部１１０は、予め定められたポリシに従いパケットを廃棄する、又は、パケットを全てのネットワークインタフェース部から送信する。

【００４０】

図１１は、パケット処理部５１０の処理の詳細説明図である。

パケット処理部５１０は、ネットワークインタフェース部ａ１２１～ｅ１２５からパケットを受け取ると、受け取ったパケットの中からフィルタリング対象となるアドレス部を抽出する（Ｓ１０１、Ｓ１０２）。この例では、パケット処理部５１０は、受け取ったパケットから、宛先ＭＡＣアドレスと送信元ＭＡＣアドレスと送信元ＩＰｖ６アドレスをそれぞれ同時に抽出することを示すが、これに限られず適宜の方法により、フィルタリング対象となる複数個の情報を抽出してもよい。

【００４１】

次に、パケット処理部５１０は、例えば、図８に示すようなフィルタリングテーブル５２０を参照して、抽出したアドレス部とフィルタリングテーブル５２０をそれぞれ比較し、比較結果として中継又は廃棄を示す情報を取得する（Ｓ１０３、Ｓ１０４）。パケット処理部５１０は、取得した比較結果のＡＮＤ条件（Ｓ１０５）により、比較結果の全てが「中継」だった場合、入力したパケットをパ

ケット中継部１１０へ送り、一方、比較結果の一つでも「廃棄」だった場合、入力したパケットを廃棄する（Ｓ１０６）。

【００４２】

また、パケット処理部５１０は、ステップＳ１０１、Ｓ１０２で抽出したアドレス部とフィルタリングテーブル５２０をそれぞれ比較し、各アドレスのＡＮＤ条件により一括して中継又は廃棄を示す情報を取得してもよい。すなわち、ＭＡＣフィルタリングとＩＰｖ６フィルタリングを独立に行うこともできるし、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、送信元ＩＰｖ６アドレスのＡＮＤ条件により、中継又は廃棄を判断する一括フィルタリング方式とすることもできる。

【００４３】

図１２は、フィルタリング処理部１３１～１３５の他の構成図である。図１２に示すフィルタリング処理部１３１～１３５は、ＭＡＣフィルタリング、ＩＰｖ６フィルタリングを順番に行うパイプライン型フィルタリング処理部である。フィルタリング処理部１３１～１３５は、それぞれＭＡＣアドレス処理部５３０、ＩＰｖ６アドレス処理部５４０、ＭＡＣアドレスフィルタリングテーブル５５０、ＩＰｖ６アドレスフィルタリングテーブル５６０を備える。上述のフィルタリング処理部１３１～１３５が、複数のパラメータを並行してチェックする並行フィルタリング方式であるのに対して、図１２に示すフィルタリング処理部１３１～１３５は、ＭＡＣアドレス、ＩＰｖ６アドレスを別個にチェックする２段フィルタリング方式である。

【００４４】

ＭＡＣアドレス処理部５３０は、ネットワークインタフェース部ａ１２１～ｅ１２５からパケットを受け取ると、受け取ったパケットから宛先アドレスと送信元ＭＡＣアドレスを抽出し、ＭＡＣアドレスフィルタリングテーブル５５０を参照してパケットの「中継」又は「廃棄」を判断する。ＭＡＣアドレス処理部５３０は、パケットの「中継」と判断した場合、受け取ったパケットをＩＰｖ６アドレス処理部５４０へ送り、一方、パケットの「廃棄」と判断した場合、受け取ったパケットを廃棄する。

【００４５】

ＩＰｖ６アドレス処理部５４０は、ＭＡＣアドレス処理部５３０からパケットを受け取ると、受け取ったパケットから宛先アドレスと送信元ＩＰｖ６アドレスを抽出し、ＩＰｖ６アドレスフィルタリングテーブル５６０を参照してパケットの「中継」又は「廃棄」を判断する。ＩＰｖ６アドレス処理部５３０は、パケットの「中継」と判断した場合、受け取ったパケットをパケット中継部１１０へ送り、一方、パケットの「廃棄」と判断した場合、受け取ったパケットを廃棄する。なお、図１２に示すフィルタリング処理部５１０は、ＭＡＣアドレス、ＩＰｖ６アドレスの順にフィルタリングしているが、逆の順にフィルタリングする構成としてもよい。

【００４６】

図１３は、ＭＡＣアドレスフィルタリングテーブル５５０及びＩＰｖ６アドレスフィルタリングテーブル５６０の構成図である。ＭＡＣアドレスフィルタリングテーブル５５０、及び、ＩＰｖ６アドレスフィルタリングテーブル５６０は、図８に示すフィルタリングテーブル５２０の送信元ＭＡＣアドレスフィールド６２１と送信元ＩＰｖ６アドレスフィールド６２２を独立して構成したテーブルである。図１３（ａ）に示すＭＡＣアドレスフィルタリングテーブル５５０は、宛先アドレス条件フィールド６１０、送信元ＭＡＣアドレス条件フィールド６２１、中継／廃棄フラグフィールド６３０を含む。図１３（ｂ）に示すＩＰｖ６アドレスフィルタリングテーブル５６０は、宛先アドレス条件フィールド６１０、送信元ＩＰｖ６アドレス条件フィールド６２２、中継／廃棄フラグフィールド６３０を含む。なお、送信元ＩＰｖ６アドレスフィールド６２２には、ＩＰｖ６インタフェースＩＤが登録されてもよい。また、宛先アドレスフィールド６１０には、ＩＰｖ６アドレスが登録されてもよい。

【００４７】

ＭＡＣアドレスフィルタリングテーブル５５０及びＩＰｖ６アドレスフィルタリングテーブル５６０は、図８又は図９に示すフィルタリングテーブル５２０と同様の構成として一つのテーブルとすることもできる。この場合、ＭＡＣアドレス処理部５３０及びＩＰｖ６アドレス処理部５４０は、送信元アドレスフィールド６２０のＭＡＣアドレス又はＩＰｖ６アドレスのいずれかを参照して、パケッ

トの「中継」又は「廃棄」を判断する。

【００４８】

２．広域イーサネット（登録商標）への適用事例及び動作例

図１４は、広域イーサネット（登録商標）網におけるネットワーク認証システムの構成図である。図１４に示すシステムは、通信事業者が提供している広域イーサネット（登録商標）網を使用して、企業等が社内イントラネットを構築した事例である。広域イーサネット（登録商標）網サービスは、通常ＬＡＮスイッチ（Ｌ２スイッチ）で構成したＬ２サービスを提供しており、各サイトは、フルメッシュでそれぞれのサイトが接続されているように動作する。以下、本実施の形態におけるネットワーク認証システムの動作例を、広域イーサネット（登録商標）網を用いて説明する。

【００４９】

ネットワーク認証システムは、サイトＡ～Ｄが広域イーサネット（登録商標）網６００を介してすべてＬ２で結ばれており、あたかも全体が構内ＬＡＮのように動作する。サイトＡは、回線終端装置６１０を介して広域イーサネット（登録商標）網６００に接続されているネットワークノード１００と、認証サーバ２００と、ファイルサーバ（情報サーバ）３００を備える。また、ネットワークノード１００は、パケット中継部１１０、ネットワークインタフェース部ａ１２１～ｅ１２５、フィルタリング処理部１３１～１３５、ファイル変更指示処理部１４０、ＩＰｖ６処理部１５０、アドレステーブル１６０を有する。フィルタリング処理部１３１～１３５は、ＭＡＣアドレス処理部５３０及びＩＰｖ６アドレス処理部５４０を備えてもよい。

【００５０】

サイトＤは、回線終端装置６２０を介して広域イーサネット（登録商標）網６００に接続されているユーザ端末４００を有する。サイトＢ及びＣは、回線終端装置を介して広域イーサネット（登録商標）網６００に接続され、例えば、ネットワークノード、ＬＡＮスイッチ、ユーザ端末、認証サーバ、ファイルサーバ等を有する。

【００５１】

サイトＡでは、例えば、広域イーサネット（登録商標）網６００はネットワークノード１００のネットワークインタフェース部ｂ１２２に、認証サーバ２００はネットワークインタフェース部ｃ１２３に、ファイルサーバ３００はネットワークインタフェース部ｄ１２４に、それぞれ接続されている。また、ネットワークノード１００の広域イーサネット（登録商標）網６００側と認証サーバ２００、ファイルサーバ３００側は全て同一ＩＰサブネットアドレスが割り当ててある。従って、ＩＰサブネットをまたぐときに使うルータは不要である。

【００５２】

サイトＣ及びサイトＤのユーザ端末は、広域イーサネット（登録商標）網６００を介してサイトＡのファイルサーバ３００にアクセス可能である。この場合、ユーザ認証は、ユーザ端末（Ｅｎｄシステム）とサイト単位で行われる。例えば、サイトＡの認証サーバ２００で認証されたユーザ端末は、サイトＡ内の全てのサーバにアクセス可能となる。

【００５３】

なお、広域イーサネット（登録商標）ではVLAN-Tag付きイーサネット（登録商標）パケットが広く使われている。フィルタリング処理部１３１～１３５は、標準イーサネット（登録商標）だけでなくVLAN-Tag付きイーサネット（登録商標）パケットもフィルタリング可能である。

【００５４】

次に、サイトＤのユーザ端末４００が、サイトＡのファイルサーバ３００だけをアクセス可能とする場合について説明する。サイトＡとサイトＤはＶＬＡＮ(Virtual LAN)１、サイトＡ、Ｂ、ＣはＶＬＡＮ２として予め設定されている。また、ネットワークノード１００の広域イーサネット（登録商標）６００側のフィルタリング処理部１３２には、例えば、図８に示すようなフィルタリングテーブルが登録されている。例えば、ブロードキャストアドレス(FF:FF:FF:FF:FF:FF)、自ネットワークノード１００(22:22:00:FF:FF:FF)、認証サーバ２００(22:22:00:11:11:11)を宛先とするパケットのみ中継するように構成されている。また、ネットワークノード１００の認証サーバ側、ファイルサーバ側のフィルタリング処理部１３３及び１３４のテーブルには何も登録されていない。

【００５５】

まず、サイトＤのユーザ端末４００が、ＩＰｖ６アドレスを生成する処理について説明する。ユーザ端末４００は、広域イーサネット（登録商標）網６００に接続されると、ネットワークＩＤを取得するために「ルータ要請コマンド」をブロードキャストする。この時、ルータ要請コマンドを含むパケットの宛先ＭＡＣアドレスは、ブロードキャストアドレス(FF:FF:FF:FF:FF:FF)として送信される。ブロードキャストされたルータ要請コマンドは、ＶＬＡＮ１で制限されてサイトＡだけに届く。

【００５６】

サイトＡのネットワークノード１００のフィルタリング処理部１３２は、ネットワークインタフェース部ｂ１２２を介して、ルータ要請コマンドを含むパケットを受け取る。フィルタリング処理部１３２のＭＡＣアドレス処理部５３０は、受け取ったパケットの宛先ＭＡＣアドレス及び送信元ＭＡＣアドレスに基づき、フィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。宛先ＭＡＣアドレスがブロードキャストアドレス、送信元ＭＡＣアドレスがユーザ端末４００と一致するエントリは＃３及び＃４であり、ＭＡＣアドレス処理部５３０は、テーブルの上位にある＃３のエントリを参照する。＃３のエントリの中継／廃棄フラグフィールド６３０はパケットの「中継」を示している。したがって、ＭＡＣアドレス処理部５３０は、当該パケットをＩＰｖ６アドレス処理部５４０へ送る。

【００５７】

ＩＰｖ６アドレス処理部５４０は、パケットを受け取ると、宛先ＭＡＣアドレス及び送信元ＩＰｖ６アドレスに基づきフィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。宛先ＭＡＣアドレスがブロードキャストアドレス、送信元ＩＰｖ６アドレスがユーザ端末４００と一致するエントリは＃３及び＃４である。テーブルの上位のエントリ＃３の中継／廃棄フラグフィールド６３０はパケットの「中継」を示している。したがって、ＩＰｖ６アドレス処理部５４０は、パケットの中継と判断し、当該パケットをパケット中継部１１０へ送る。

【００５８】

パケット中継部１１０は、フィルタリング処理部１３２からパケットを受け取ると、まず、アドレステーブル１６０を参照し、送信元ＭＡＣアドレスが一致するエントリが存在するか検索する。なお、アドレステーブル１６０には、図１０に示すエントリが予め登録されている。パケット中継部１１０は、該当するエントリがアドレステーブル１６０にない場合、送信元ＭＡＣアドレス及びルータ要請コマンドを受け取ったネットワークインタフェース部の識別子をアドレステーブル１６０に追加する。

【００５９】

図１５は、ユーザ端末４００のエントリが追加されたアドレステーブル１６０の構成図である。図１０に示すアドレステーブル１６０には、送信元であるユーザ端末４００のＭＡＣアドレス(22:22:FF:00:00:01)と一致するエントリがないため、パケット中継部１１０は、ユーザ端末４００のＭＡＣアドレス(22:22:FF:00:00:01)とパケットを受信したネットワークインタフェースｂ１２２の識別子「ｂ」を含むエントリを追加する。

【００６０】

次に、パケット中継部１１０は、アドレステーブル１６０を参照し、宛先ＭＡＣアドレスが一致するエントリが存在するか検索し、パケットを中継するネットワークインタフェース部の識別子を取得する。アドレステーブル１６０には、ブロードキャストアドレス(FF:FF:FF:FF:FF:FF)のエントリがあるので、パケット中継部１１０は、中継先として「ｘ」を取得する。パケット中継部１１０は、取得した中継先が「ｘ」であるので、受け取ったルータ要請コマンドをＩＰｖ６処理部１５０へ中継する。

【００６１】

ＩＰｖ６処理部１５０は、ルータ要請コマンドを受け取ると、ルータ通知コマンドを使い、ユーザ端末４００(22:22:FF:00:00:01)を宛先としてネットワークＩＤを含むパケットをパケット中継部１１０に送る。パケット中継部１１０は、上述と同様に、アドレステーブル１６０を参照して、宛先ＭＡＣアドレスが一致するエントリを検索する。図１５に示すように、宛先であるユーザ端末のアドレ

スのエントリは既に登録されており、パケット中継部１１０は、中継先としてネットワークインタフェース部の識別子「ｂ」を取得する。パケット中継部１１０は、取得した中継先「ｂ」に従い、ネットワークＩＤを含むパケットをネットワークインタフェース部ｂ１２２を介して、ユーザ端末４００に中継する。

【００６２】

ユーザ端末４００は、ネットワークＩＤを受信し、受信したネットワークＩＤと自ＭＡＣアドレスに基づいて自ＩＰｖ６アドレスを作成する。ユーザ端末４００は、ＩＰｖ６アドレス作成の後に、サイトＡのネットワークノード１００に対するユーザ認証を行う。

【００６３】

図１６は、サイトＤのユーザ端末４００が、サイトＡのファイルサーバ３００にアクセスするシーケンス図である。まず、ユーザ端末４００が、ユーザ認証を受けずにファイルサーバ３００にアクセスを試みた場合の処理について説明する。

【００６４】

例えば、サイトＤのユーザ端末４００から、宛先ＭＡＣアドレスをファイルサーバ３００(22:22:00:22:22:22)とするパケットが送信されたとする（Ｓ２０１）。ネットワークノード１００のフィルタリング処理部１３２は、ネットワークインタフェース部ｂ１２２を介してファイルサーバ３００宛のパケットを受け取る。フィルタリング処理部１３２のＭＡＣアドレス処理部５３０は、受け取ったパケットの宛先ＭＡＣアドレス及び送信元ＭＡＣアドレスに基づき、図８に示すフィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。宛先ＭＡＣアドレスがファイルサーバ３００(22:22:00:22:22:22)、送信元ＭＡＣアドレスがユーザ端末４００と一致するエントリは＃４であり、中継／廃棄フラグフィールド６３０はパケットの「廃棄」を示している。したがって、ＭＡＣアドレス処理部５３０は、当該パケットを廃棄する。このようにして、ユーザ認証を受けていないユーザ端末４００からファイルサーバ３００へのアクセスは拒否される。

【００６５】

次に、ユーザ認証について説明する。まず、ユーザ端末４００は、宛先ＭＡＣアドレスを認証サーバ２００(22:22:00:11:11:11)とする認証要求パケットを送信する（Ｓ２０３）。ネットワークノード１００のフィルタリング処理部１３２は、ネットワークインタフェース部ｂ１２２を介して認証サーバ２００宛のパケットを受け取る。フィルタリング処理部１３２のＭＡＣアドレス処理部５３０は、上述と同様にフィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。宛先ＭＡＣアドレスが認証サーバ２００(22:22:00:11:11:11)、送信元ＭＡＣアドレスがユーザ端末４００であるので、ＭＡＣアドレス処理部５３０は、エントリは＃１のエントリを参照し、パケットをＩＰｖ６アドレス処理部５４０へ送る（Ｓ２０５）。

〔００６６〕

ＩＰｖ６処理部５４０は、パケットを受け取ると、上述と同様にフィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。宛先ＭＡＣアドレスが認証サーバ２００(22:22:00:11:11:11)、送信元ＩＰｖ６アドレスがユーザ端末４００であるので、ＩＰｖ６アドレス処理部５４０は、エントリは＃１のエントリを参照し、当該パケットをパケット中継部１１０へ送る。

〔００６７〕

パケット中継部１１０は、パケットを受け取るとアドレステーブル１６０を参照し、送信元ＭＡＣアドレスが一致するエントリが存在するか検索する。図１５に示すようにアドレステーブル１６０には、既にユーザ端末４００(22:22:FF:00:00:01)のエントリが存在するので、次の処理へ移る。

〔００６８〕

次に、パケット中継部１１０は、宛先ＭＡＣアドレス(22:22:00:11:11:11)に基づいてアドレステーブル１６０を参照し、中継先として「ｃ」を取得する。パケット中継部１１０は、中継先「ｃ」に従い、ネットワークインタフェース部ｃ１２３を介して当該認証要求パケットを認証サーバ２００に中継する（Ｓ２０７）。このように、フィルタリングテーブル５２０が中継を示すパケットは、宛先アドレスへ中継される。

〔００６９〕

認証サーバ２００は、認証要求パケットを受け取ると、宛先ＭＡＣアドレスをユーザ端末４００(22:22:FF:00:00:01)として、ユーザ認証に必要な認証パラメータの要求パケットを送信する（Ｓ２０９）。

【００７０】

認証サーバ２００から送信されたパケットは、ネットワークインタフェース部ｃ１２３を介して、フィルタリング処理部１３３に送られる。パケットを受け取ったフィルタリング処理部１３３のＭＡＣアドレス処理部５３０は、フィルタリングテーブル５２０を参照する。フィルタリング処理部１３２のフィルタリングテーブル５２０には何も登録されていないため、ＭＡＣアドレス処理部５３０は、ＩＰｖ６アドレス処理部５４０へパケットを送る（Ｓ２１１）。ＩＰｖ６アドレス処理部５４０も同様に、パケットをパケット中継部１１０へ送る。パケット中継部１１０は、上述と同様にアドレステーブル１６０を参照し、宛先であるユーザ端末のＭＡＣアドレス(22:22:FF:00:00:01)に対応する中継先として「ｂ」を取得する。パケット中継部１１０は、ネットワークインタフェース部ｂ１２２を介してパケットをユーザ端末４００に中継する（Ｓ２１３）。

【００７１】

認証パラメータの要求パケットを受信したユーザ端末４００は、要求された認証パラメータを含むパケットを、認証サーバ２００宛に送信する（Ｓ２１５）。認証パラメータとしては、例えば、ユーザＩＤ、パスワード、ＭＡＣアドレス、ＩＰｖ６インタフェースＩＤ（図
中、ＩＰｖ６－ｉｆＩＤと記す）、ＩＰｖ６アドレス等の組み合わせ又はいずれかである。

【００７２】

ネットワークノード１００のフィルタリング処理部１３２は、ネットワークインタフェース部ｂ１２２を介して認証サーバ２００宛のパケットを受け取る。フィルタリング処理部１３２のＭＡＣアドレス処理部５３０及びＩＰｖ６アドレス処理部５４０は、上述のステップＳ２０５及びＳ２０７の認証要求パケットの中継と同様の処理を行い、ネットワークインタフェース部ｃ１２３から当該パケットを認証サーバ２００に中継する（Ｓ２１７、Ｓ２１９）。

【００７３】

認証サーバ２００は、認証パラメータを含むパケットを受信すると、受信した認証パラメータと予め格納されている認証用データとを比較し、ユーザ認証を行う。ユーザ認証のパラメータとしてユーザＩＤとパスワードの他にＭＡＣアドレス、ＩＰｖ６インタフェースＩＤを使用し、ユーザ認証の正確性を高めている。ユーザ認証がされると、認証サーバ２００は、ネットワークノード１００のフィルタ変更指示処理部１４０と通信し、状態変更指示を送信する（Ｓ２２１）。状態変更指示は、例えば、宛先アドレスの内容として「任意」、送信元アドレスの内容として認証したユーザ端末４００のＭＡＣアドレス(22:22:FF:00:00:01)及びＩＰｖ６アドレス(2001:200:0:1:2222:FFFF:FE00:1)、パケットの「中継」を示すフラグ、エントリの追加を示すフラグを含む。

【００７４】

図１７は、状態変更指示に従い変更されたフィルタリングテーブル５２０の構成図である。フィルタ変更指示処理部１４０は、認証サーバ２００から状態変更指示を受け取ると、状態変更指示に含まれるユーザ端末４００のＭＡＣアドレス(22:22:FF:00:00:01)に基づきアドレステーブル１６０を参照し、そのＭＡＣアドレスに対応するネットワークインタフェース部の識別子「ｂ」を取得する。次に、フィルタ変更指示処理部１４０は、取得した識別子が「ｂ」であるので、ネットワークインタフェース部ｂ１２２に対応するフィルタリング処理部１３２のフィルタリングテーブル５２０を状態変更指示に従い変更する。図１７に示すように、認証サーバ２００から送信された状態変更指示に応じたエントリが＃１に追加される。このエントリが追加されることで、ユーザ端末４００からファイルサーバ３００等のネットワークノード１００に接続されている機器へのパケットは中継されることになる。

【００７５】

なお、認証サーバ２００は、状態変更指示を含むパケットをネットワークノード１００宛てに送信し、パケット中継部１１０は、受け取ったパケットが状態変更指示であるか判断してパケットを中継するように構成してもよい。例えば、自ＭＡＣアドレス宛のパケットが、状態変更指示を含む場合、受け取ったパケット

をフィルタ変更指示処理部１４０に中継し、一方、ルータ要請コマンドの場合、受け取ったパケットをＩＰｖ６処理部１５０に中継するように構成してもよい。

【００７６】

ユーザ認証が完了した後、ユーザ端末４００は、宛先ＭＡＣアドレスをファイルサーバ３００(22:22:00:22:22:22)とするパケット（例えば、ファイルのＲｅａｄ要求）を送信する（Ｓ２２３）。

【００７７】

ネットワークノード１００のフィルタリング処理部１３２は、ネットワークインタフェース部ｂ１２２を介してファイルサーバ３００宛のパケットを受け取り、パケットの中継又は廃棄を判断する。送信元ＭＡＣアドレス(22:22:FF:00:00:01)、及び、送信元ＩＰｖ６アドレス(2001:200:0:1:2222:FFFF:FE00:1)のエントリがフィルタリングテーブル５２０の＃１に存在するため、フィルタリング処理部１３２のＭＡＣアドレス処理部５３０は、ＩＰｖ６アドレス処理部５４０へパケットを中継し（Ｓ２２５）、ＩＰｖ６アドレス処理部５４０は、パケット中継部１１０へパケットを中継する。

【００７８】

パケット中継部１１０は、アドレステーブル１６０を参照し、送信元ＭＡＣアドレスが一致するエントリが存在するか検索する。アドレステーブル１６０には、既にユーザ端末４００のエントリが存在するので、次の処理へ移る。パケット中継部１１０は、宛先ＭＡＣアドレス(22:22:00:22:22:22)に基づいてアドレステーブル１６０を参照し、中継先として「ｄ」を取得する。パケット中継部１１０は、取得した中継先に従い、ネットワークインタフェース部ｄ１２４を介して当該パケットをファイルサーバ３００に中継する（Ｓ２２７）。

【００７９】

ファイルサーバ３００は、要求されたデータをユーザ端末４００宛に送信する（Ｓ２２９）。送信されたデータは、ネットワークノード１００のフィルタリング処理部１３４に送られる。フィルタリング処理部１３４は、上述のステップＳ２１１及びＳ２１３と同様の処理を行い、データをユーザ端末４００へ中継する（Ｓ２３１、Ｓ２３３）。

【００８０】

なお、不正なユーザ端末から同一ＩＰになりすましてファイルサーバ３００にパケットが送信された場合、ＭＡＣアドレス処理部５３０でのＭＡＣフィルタリングにより、当該パケットは廃棄される（Ｓ２５１）。

【００８１】

上述の実施の形態では、ＭＡＣアドレス処理部５３０とＩＰｖ６アドレス処理部５４０により、２段フィルタリングを行っているが、並行してフィルタリングする並行フィルタリング、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、及び、送信元ＩＰｖ６アドレスに基づく、一括フィルタリングを行うこともできる。また、上述の実施の形態では、ＭＡＣアドレス及びＩＰｖ６アドレスによりフィルタリングしているが、図９に示すようなフィルタリングテーブル５２０を用いて、ＭＡＣアドレス及びＩＰｖ６インタフェースＩＤによりフィルタリングすることもできる。

【００８２】

なお、サイトＤのユーザ端末がサイトＡのファイルサーバにアクセスする場合等、いずれかのサイトに属するユーザ端末が、他のサイトのファイルサーバにアクセスする場合も、上述と同様の処理によりアクセスが可能となる。

【００８３】

また、宛先アドレスは、ＭＡＣアドレスを用いる以外にも、ＩＰｖ６アドレスを用いることもできる。この場合、アドレステーブル１６０は、ＩＰアドレスに対応してネットワークインタフェース部の識別子を登録すればよい。

【００８４】

さらに、認証サーバ２００とファイルサーバ３００を同一ＩＰアドレスにしてユーザ端末４００からは１台のように見せることもできる。最初にユーザ端末４００は認証サーバ２００に対してユーザ認証を受けるが、認証後、同一ＩＰアドレスを使ってファイルサーバ３００にアクセスすることを可能にする。そのためにネットワークノード１００は、認証前は認証サーバ２００に、認証後はファイルサーバ３００にパケットを転送する仕掛けを用意する。例えば、ユーザ認証を受けたＩＰアドレス等を記憶するためのアドレス登録表を用意する。同一ＩＰア

ドレスにすると、ネットワークノードと認証サーバ、ファイルサーバが１台の装置で動いているように見える。従来技術では１台の実サーバで実現する事ができるが、性能が大幅に劣化する。本実施の形態におけるネットワーク認証システムは、このトラフィック性能に対する向上策でもある。

【００８５】

３．構内データセンタへの適用事例及び動作例

図１８は、構内データセンタにネットワークノードを適用したネットワーク認証システムの構成図である。図１８に示すネットワーク認証システムは、データセンタ７００と、認証サーバ２００と、情報コンセント７３０を介してネットワーク３に接続されたユーザ端末４００と、ルータ７１０を備える。データセンタ７００は、ファイルサーバ３００とネットワークノード１００を有する。データセンタ７００、認証サーバ２００、ユーザ端末４００は、それぞれネットワーク１、２、３に接続され、ルータ７１０を介して通信可能である。また、情報コンセント７３０を増やすためのＬＡＮスイッチ７２０を備えてもよい。

【００８６】

ネットワーク１～３は、それぞれ別のＩＰサブネットになっており、これらはルータ７１０を介して通信される。ユーザ端末４００からデータセンタ７００宛てのパケットが送信されると、ユーザ端末４００のＭＡＣアドレスは、ルータ７１０で削除されネットワークノード１００まで届かない。したがって、ネットワークノード１００では、ＭＡＣフィルタリングをすることができない。また、ＩＰアドレスのなりすましに対するセキュリティ強度が低い。そこで、本実施の形態では、ネットワークノード１００は、ＩＰｖ６アドレスのインタフェースＩＤに基づき、パケットをフィルタリングする。インタフェースＩＤは、装置固有のＩＤであるため、セキュリティ強度を高くすることができる。

【００８７】

データセンタ７００は、サーバを一箇所にまとめたものであり、ユーザ端末４００に対してｗｅｂサービスをはじめとする各種サービスを提供する。なお、サーバは、論理的に集中されていれば、物理的に離れていてもよい。サーバとネットワーク１の出入り口は１箇所に絞り、ここにネットワークノード１００を配置

し、特定のユーザ端末４００のみ構内へのアクセスを可能にする。特定のユーザ端末４００からのみサーバにアクセスさせることで、サーバをＤｏＳ(Denial of Service)アタックから守る事ができる。また、ネットワークノード１００に認証の仕組みを持たせることで、サーバ毎に認証の仕組みを有する必要がなくなる。

【００８８】

図１９は、フィルタリングテーブル５２０の構成例（３）を示す図である。フィルタリングテーブル５２０は、エントリ毎に宛先ＩＰｖ６アドレス条件フィールド６１１、送信元ＩＰｖ６インタフェースＩＤ条件フィールド６２３、中継／廃棄フラグフィールド６３０を含む。図１９（ａ）に示すフィルタリングテーブル５２０は、ネットワークノード１００のネットワーク１側のフィルタリング処理部１３４に登録されている。なお、ネットワークノード１００のファイルサーバ３００側のフィルタリング処理部１３１及び１３２には、テーブルが何も登録されていない。

【００８９】

図２０は、アドレステーブル１６０の構成例（２）を示す図である。図２０（ａ）に示すように、ファイルサーバ３００、自ネットワークノード１００に関するエントリが予めネットワークノード１００のアドレステーブル１６０に登録されている。

【００９０】

図２１は、ユーザ端末４００がデータセンタ７００内のファイルサーバ３００にアクセスするシーケンス図である。

【００９１】

まず、ユーザ端末４００は、情報コンセント７３０を介してネットワーク３に接続されると、ネットワークＩＤを取得するために「ルータ要請コマンド」をルータ７１０に送信する（Ｓ３０１）。なお、ユーザ端末４００は、宛先をブロードキャストアドレスとして、「ルータ要請コマンド」を送信してもよい。ルータ７１０は、ユーザ端末４００からの「ルータ要請コマンド」を受け取ると、ルータ通知コマンドを使い、ユーザ端末４００にネットワークＩＤを通知する（Ｓ３０

３）。ユーザ端末４００は、ネットワークＩＤを受信し、受信したネットワークＩＤと自ＭＡＣアドレスに基づいて自ＩＰｖ６アドレスを作成する。

【００９２】

ここで、ユーザ端末４００から、宛先ＩＰｖ６アドレスがファイルサーバ３００(2001:200:0:3:2222:00FF:FE22:2222)とするパケットが送信された場合（Ｓ３０５）について説明する。ルータ７１０は、ユーザ端末４００からのパケットを受け取り、ファイルサーバ３００が属するネットワーク１にルーティングする（Ｓ３０７）。この時、パケットに含まれていたユーザ端末のＭＡＣアドレスは、ルータ７１０によって削除される。

【００９３】

ネットワークノード１００のフィルタリング処理部１３４は、ネットワークインタフェース部ｄ１２４を介してファイルサーバ３００宛のパケットを受け取る。フィルタリング処理部１３４は、受け取ったパケットから、宛先ＩＰｖ６アドレス及び送信元ＩＰｖ６アドレスのインタフェースＩＤを抽出する。次に、フィルタリング処理部１３４は、宛先ＩＰｖ６アドレス及び送信元ＩＰｖ６インタフェースＩＤに基づき、図１９に示すフィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。宛先ＩＰｖ６アドレスがファイルサーバ３００、送信元ＩＰｖ６インタフェースＩＤがユーザ端末４００と一致するエントリは＃１であり、中継／廃棄フラグフィールド６３０はパケットの「廃棄」を示している。したがって、フィルタリング処理部５１０は、パケットの廃棄と判断し、当該パケットを廃棄する。このようにして、ユーザ認証を受けていないユーザ端末４００からファイルサーバ３００へのアクセスは拒否される。

【００９４】

次に、ユーザ認証について説明する。まず、ユーザ端末４００は、宛先ＩＰｖ６アドレスを認証サーバ２００(2001:200:0:2:2222:00FF:FE11:1111)とする認証要求パケットを送信する（Ｓ３０９）。ルータ７１０は、ネットワーク３を介して認証要求パケットを受け取り、宛先ＩＰｖ６アドレスに基づいて、認証要求パケットをネットワーク２へルーティングする（Ｓ３１１）。

【００９５】

認証サーバ２００は、ネットワーク２を介して認証要求パケットを受け取ると、宛先ＩＰｖ６アドレスをユーザ端末４００(2001:200:0:1:2222:FFFF:FE00:1)として、ユーザ認証に必要な認証パラメータの要求パケットを送信する（Ｓ３１３）。ルータ７１０は、認証パラメータの要求パケットを受け取り、宛先ＩＰｖ６アドレスに基づいて、受け取ったパケットをネットワーク３へルーティングする（Ｓ３１５）。

【００９６】

ネットワーク３を介して認証パラメータの要求パケットを受信したユーザ端末４００は、認証パラメータを含むパケットを、認証サーバ２００宛に送信する（Ｓ３１７）。認証パラメータとしては、例えば、ユーザＩＤ、パスワード、及び、ＩＰｖ６インタフェースＩＤである。

【００９７】

認証サーバ２００は、ルータ７１０を介して、ユーザ端末４００から送信された認証パラメータを含むパケットを受信する（Ｓ３１９）。次に、認証サーバ２００は、受信した認証パラメータと予め格納されている認証用データとを比較し、ユーザ認証を行う。ユーザ認証がされると、認証サーバ２００は、ネットワークノード１００のフィルタ変更指示処理部１４０と通信し、フィルタ変更指示処理部１４０に状態変更指示を送信する（Ｓ３２１）。状態変更指示は、例えば、宛先アドレスの内容が「任意」、認証したユーザ端末４００のＩＰｖ６インタフェースＩＤ(2222:FFFF:FE00:1)、パケットの「中継」を示すフラグ、エントリの追加を示すフラグを含む。

【００９８】

ネットワークノード１００のフィルタ変更指示処理部１４０は、ルータ７１０、及び、ネットワークインタフェース部ｄ１２４を介して、認証サーバ２００から送信された状態変更指示を受信する（Ｓ３２３）。

【００９９】

フィルタ変更指示処理部１４０は、状態変更指示を受け取ると、ネットワーク１が接続されているネットワークインタフェース部ｂ１２４に対応するフィルタリング処理部１３２のフィルタリングテーブル５２０を状態変更指示に従い変更

する。図１９（ｂ）に示すように、認証サーバ２００から送信された状態変更指示に応じたエントリが＃１に追加される。このエントリが追加されることで、ユーザ端末４００からファイルサーバ３００へのパケットは中継されることになる。

【０１００】

ユーザ認証が完了した後、ユーザ端末４００は、宛先ＩＰｖ６アドレスをファイルサーバ３００(2001:200:0:1:2222:00FF:FE22:2222)とするパケット（例えば、ファイルのＲｅａｄ要求）を送信する（Ｓ３２５）。ルータ７１０は、宛先ＩＰｖ６アドレスに基づき、パケットをネットワーク１へルーティングする（Ｓ３２７）。

【０１０１】

ネットワークノード１００のフィルタリング処理部１３４は、ネットワークインタフェース部ｄ１２４を介してファイルサーバ３００宛のパケットを受け取る。次に、フィルタリング処理部１３４は、上述と同様に受け取ったパケットの宛先ＩＰｖ６アドレス、及び、送信元ＩＰｖ６インタフェースＩＤに基づき、フィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。図１９（ｂ）に示すように、フィルタリングテーブルの＃１及び＃３に該当するエントリが存在するため、フィルタリング処理部１３４は、テーブルの上位に存在する＃１のエントリの中継／廃棄フラグフィールド６３０を参照し、パケットの中継と判断する。フィルタリング処理部１３４は、受け取ったパケットを、パケット中継部１１０へ送る。

【０１０２】

パケット中継部１１０は、フィルタリング処理部１３４からパケットを受け取ると、アドレステーブル１６０を参照し、送信元ＭＡＣアドレスが一致するエントリが存在するか検索する。図２０（ａ）に示すアドレステーブル１６０には、送信元であるユーザ端末４００のＩＰｖ６インタフェースＩＤ(2222:FFFF:FE00:1)と一致するエントリがないため、パケット中継部１１０は、ユーザ端末４００のＩＰｖ６インタフェースＩＤとネットワーク１に接続されているネットワークインタフェースｄ１２４の識別子「ｄ」を含むエントリを追加する。図２０（ｂ

）に、ユーザ端末４００のエントリが追加されたアドレステーブル１６０の構成図を示す。

【０１０３】

次に、パケット中継部１１０は、宛先ＩＰｖ６インタフェースＩＤ(2222:00FF:FE22:2222)に基づいてアドレステーブル１６０を参照し、中継先として「ａ」を取得する。パケット中継部は、取得した中継先に従い、ネットワークインタフェース部ａ１２１を介して当該パケットをファイルサーバ３００に中継する（Ｓ３２９）。

【０１０４】

ファイルサーバ３００は、ユーザ端末４００からのパケットの内容に従い、ユーザ端末４００(2001:200:0:1:2222:FFFF:FE00:1)を宛先とするパケットを送信する（Ｓ３３１）。

【０１０５】

ファイルサーバ３００から送信されたパケットは、ネットワークインタフェース部ａ１２１を介して、フィルタリング処理部１３１に送られる。パケットを受け取ったフィルタリング処理部１３１は、フィルタリングテーブル５２０を参照する。フィルタリング処理部１３２のフィルタリングテーブル５２０には何も登録されていないため、フィルタリング処理部１３１は、パケット中継部１１０へパケットを送る。

【０１０６】

パケット中継部１１０は、上述と同様に、宛先ＩＰｖ６インタフェースＩＤアドレス(2222:FFFF:FE00:1)に基づいてアドレステーブル１６０を参照し、中継先として「ｄ」を取得する。パケット中継部は、取得した「ｄ」に従い、ネットワークインタフェース部ｄ１２４を介して、当該パケットをユーザ端末４００に送信する（Ｓ３３３）。ユーザ端末４００は、ルータ７１０を介して、ファイルサーバ３００から送信されたパケットを受信する（Ｓ３３５）。なお、ユーザ端末４００は、ユーザ認証を１度受けると、構内データセンタ７００内の他のファイルサーバへもアクセスすることができる。

【０１０７】

また、不正なユーザ端末（侵入者）からファイルサーバ３００にアクセスをしようとした場合（Ｓ３５１）、端末からのパケットはルータ７１０により送信元ＭＡＣアドレスが削除されルーティングされるが（Ｓ３５３）、フィルタリング処理部１３４でのＩＰｖ６インタフェースＩＤに基づくフィルタリングにより、当該パケットは廃棄される。

【０１０８】

このように、不正なユーザ端末からのアクセスを拒否することにより、ファイルサーバ３００をＤｏＳアタックから守ることができる。また、サーバそのもの認証の仕組みを持つ必要がなく、管理も容易である。

【０１０９】

４．インターネットＶＰＮの事例

図２２は、インターネットＶＰＮにおけるネットワーク認証システムの構成図である。ネットワーク認証システムは、ＩＰｓｅｃ通信が可能なネットワークノード１１００、認証サーバ２００、ファイルサーバ３００を有するサイトＥと、ＩＰｓｅｃ通信が可能なユーザ端末１４００を有するサイトＦを備える。また、サイトＥとサイトＦは、回線終端装置８１０及び８２０を介して、インターネット８００に接続されている。図２２に示す図は、通信事業者が提供するインターネット接続サービスを用いて、企業等が社内イントラネットを構築した例である。各サイトは、例えば、ＩＰｓｅｃを使ってトンネルで結ばれており、各通信パスはあたかも専用線で結ばれているように通信される。また、パケットは暗号化されて送受信される。

【０１１０】

図２３は、ＩＰｓｅｃ通信が可能なネットワークノード１１００の構成図である。ネットワークノード１１００は、パケット中継部１１０と、ネットワークインタフェース部ａ１２１～ｅ１２５と、フィルタリング処理部１３１～１３５と、フィルタ変更指示処理部１４０と、アドレステーブル１６０と、さらに、ＩＰｓｅｃ制御部１７０と、ＩＰｓｅｃ処理部１８３～１８５を備える。なお、ＩＰｓｅｃ処理部は、少なくともインターネット８００に接続されるネットワークインタフェース部に対応して備えられていればよい。例えば、図２３に示すネット

ワーク認証ノード１１００では、ネットワークインタフェース部１２３～１２５に対応して、ＩＰｓｅｃ処理部１８３～１８５を備えている。これ以外にも、全てのネットワークインタフェース部に対応してＩＰｓｅｃ処理部を備える等、適宜ＩＰｓｅｃ処理部を配置することもできる。

【０１１１】

ＩＰｓｅｃ制御部１７０は、通信相手毎にＩＫＥ(Internet Key Exchange)を用いた鍵交換処理を主に行う。ＩＰｓｅｃ制御部１７０は、ユーザ端末１４００との間で秘密対称鍵を作成し、通信パス（ＳＡ：Security Association)をインターネット８００上に自動生成する。ネットワークノード１１００とユーザ端末１４００は、ＩＰｓｅｃ制御部１７０により生成されたＳＡを介して、パケットの送受信を行う。また、ＩＰｓｅｃ制御部１７０は、ユーザ端末毎に、秘密対称鍵、ｐｒｅ－ｓｈａｒｅｄ　ｋｅｙ又は公開鍵等を記憶したキーテーブルを有する。ｐｒｅ－ｓｈａｒｅｄ　ｋｅｙは、ＩＰｓｅｃ制御部１７０とユーザ端末１４００に予め記憶された同一のｋｅｙ（パスワード）である。

【０１１２】

図２４は、キーテーブルの構成例を示す図である。例えば、ユーザ端末のＩＰｖ６アドレスフィールド、予め定められたｐｒｅ－ｓｈａｒｅｄ　ｋｅｙフィールド、通信パス生成の際に作成した秘密対称鍵フィールドを含む。キーテーブルは、これ以外にも適宜の構成とすることができる。

【０１１３】

ＩＰｓｅｃ処理部１８３～１８５は、データの暗号／復号処理（ＥＳＰ：Encapsulating Security Payload）、パケットが改ざんされていないかを確認するためのパケット認証処理（ＡＨ：Authentication Header）を主に行う。また、ＩＰｓｅｃ制御部１７０に記憶されているｐｒｅ－ｓｈａｒｅｄ　ｋｅｙ等を用いてＩＫＥにおける通信相手の認証を行う。

【０１１４】

ユーザ端末１４００は、ＩＰｓｅｃ通信が可能な端末であり、ネットワークノード１１００との間にＳＡを形成し、ＳＡを介して通信を行う。なお、パケット中継部１１０、ネットワークインタフェース部ａ１２１～ｅ１２５、フィルタリ

ング処理部１３１～１３５、フィルタ変更指示処理部１４０については、上述と同様であるので、その説明を省略する。

【０１１５】

図２５は、フィルタリングテーブル５２０の構成例（４）を示す図である。図２５（ａ）に示すフィルタリングテーブル５２０は、インターネット８００に接続されているネットワークインタフェース部１２３に対応するフィルタリング処理部１３３に登録されている。フィルタリングテーブル５２０は、各エントリ毎に、宛先ＩＰｖ６アドレス条件フィールド６１１、送信元ＩＰｖ６インタフェースＩＤ条件フィールド６２３、中継／廃棄フラグフィールド６３０を含む。

【０１１６】

図２６は、アドレステーブル１６０の構成例（３）を示す図である。例えば、アドレステーブル１６０には、認証サーバ２００、ファイルサーバ３００、自ネットワークノード１１００に関するエントリが予め登録されている。

【０１１７】

図２７は、インターネットＶＰＮにおけるネットワーク認証システムのシーケンス図である。まず、ユーザ端末１４００から、ＩＰｓｅｃを使用せずファイルサーバ宛てのパケットが送信された場合の処理について説明する。

【０１１８】

例えば、ユーザ端末１４００は、ファイルサーバ宛てのパケットを送信する（Ｓ４０１）。サイトＥのネットワークノード１１００のネットワークインタフェース部ｃ１２３は、インターネット８００を介してパケットを受け取り、ＩＰｓｅｃ処理部１８３へ送る。ＩＰｓｅｃ処理部１８３は、ＩＰｓｅｃ制御部１７０に記憶されているＰｒｅ－ｓｈａｒｅｄ　Ｋｅｙや公開鍵等を参照し、例えば、Ｐｒｅ－ｓｈａｒｅｄ　Ｋｅｙ認証や、公開鍵暗号認証、デジタル署名認証等を行う。ユーザ端末１４００から受け取ったパケットはＩＰｓｅｃ処理されていないため、ＩＫＥにおける認証を受けることができず、ＩＰｓｅｃ処理部１８３は、当該パケットを廃棄する。

【０１１９】

ここで、ＩＫＥにおけるＰｒｅ－ｓｈａｒｅｄ　Ｋｅｙを用いた認証の一例に

ついて説明する。ユーザ端末１４００は、パケットを送信する際に、予め記憶されているｐｒｅ－ｓｈａｒｅｄ　ｋｅｙと自分のＩＤ情報（例えば、ＩＰｖ６アドレス）に基づき所定の計算をした認証値もあわせて送信する。パケットを受け取ったＩＰｓｅｃ処理部１８３は、受け取ったパケットの送信元ＩＰｖ６アドレス（又は、ＩＰｓｅｃ通信装置のアドレス）に基づき、ＩＰｓｅｃ制御部１７０のキーテーブルからｐｒｅ－ｓｈａｒｅｄ　ｋｅｙを取得する。ＩＰｓｅｃ処理部１８３は、取得したｐｒｅ－ｓｈａｒｅｄ　ｋｅｙと送信元ＩＰｖ６アドレスに基づき所定の計算を行い、計算結果とユーザ端末１４００から送信された認証値を比較する。ユーザ端末１４００が、ＩＰｖ６アドレスに対応したｐｒｅ－ｓｈａｒｅｄ　ｋｅｙを使用していない場合、例えば、ｐｒｅ－ｓｈａｒｅｄ　ｋｅｙを知らない場合、比較結果は一致しない。比較結果が一致すると、ＩＰｓｅｃ処理部１８３は、パケットをフィルタリング処理部１３３へ送る。一方、比較結果が一致しない場合、ＩＰｓｅｃ処理部１８３は、パケットを廃棄する。なお、上述の認証は一例であり、これ以外にも適宜の認証方式を用いる事ができる。

【０１２０】

次に、ユーザ端末１４００が、ファイルサーバ３００にアクセスするまでの処理について説明する。まず、ユーザ端末１４００は、ネットワークノード１１００との間に、ＩＫＥによるＩＰｓｅｃ通信パスを確立する（Ｓ４０３）。

【０１２１】

例えば、ユーザ端末１４００は、制御用チャネルＩＳＡＫＭＰ(Internet security association and key management protocol)　ＳＡ生成の要求パケットをネットワークノード１１００に送信する。ネットワークノード１１００のＩＰｓｅｃ処理部１８３は、ネットワークインタフェース部１２３を介して要求パケットを受け取り、ＩＰｓｅｃ制御部１７０へ送る。ＩＰｓｅｃ制御部１７０は、要求パケットの送信元と通信受諾／拒否を示す情報が予め登録されているセキュリティポリシテーブル等を参照し、通信受諾であれば、ユーザ端末１４００に受諾通知を送信する。次に、ユーザ端末１４００及びＩＰｓｅｃ制御部１７０は、秘密対称鍵の生成、相手が通信受諾の本人であるかの認証（例えば、pre-shared key認証）を行い、ＩＳＡＫＭＰ　ＳＡ生成する。さらに、ユーザ端末１４００及

びＩＰｓｅｃ制御部１７０は、ＩＳＡＫＭＰ　ＳＡを介して通信し、秘密対称鍵の生成、実際にパケットを送受信するためのＳＡを生成する。なお、ＩＰｓｅｃ制御部１７０は、生成した秘密対称鍵をユーザ端末１４００毎に記憶する。以上の処理により、ユーザ端末１４００とネットワークノードの間にＩＰｓｅｃ通信パスが確立する。

【０１２２】

次に、ユーザ端末１４００は、宛先ＩＰアドレスを認証サーバ２００とする認証要求パケットを送信する（Ｓ４０５）。なお、サイトＥのネットワークＩＤを宛先とするユーザ端末１４００からのパケットは、ＥＳＰ機能により通信パスの確立の際に生成した秘密対称鍵を用いて暗号化され、ＩＰｓｅｃ通信パスを介して送信される。

【０１２３】

ネットワークノード１１００のネットワークインタフェース部１２３は、ＩＰｓｅｃ通信パスを介して認証要求パケットを受け取り、ＩＰｓｅｃ処理部１８３に送る。ＩＰｓｅｃ処理部１８３は、パケットを受け取ると、パケットの送信元ＩＰｖ６アドレス（又はＩＰｓｅｃ通信装置のアドレス）に基づき、ＩＰｓｅｃ制御部１７０のキーテーブルから秘密対称鍵を取得する。ＩＰｓｅｃ処理部１８３は、取得した秘密対称鍵を用いてＥＳＰ機能によりパケットを復号化する。次に、ＩＰｓｅｃ処理部１８３は、ＩＫＥにおける通信相手の認証を行う。例えば、ＩＰｓｅｃ処理部１８３は、上述のｐｒｅ－ｓｈａｒｅｄ　ｋｅｙを用いた認証を行う。通信相手を認証すると、ＩＰｓｅｃ処理部１８３は、認証要求パケットをフィルタリング処理部１３３へ送る（Ｓ４０７）。

【０１２４】

パケットを受け取ったフィルタリング処理部１３３は、パケットの宛先ＩＰｖ６アドレス、送信元ＩＰｖ６インタフェースＩＤに基づき、図２５に示すフィルタリングテーブル５２０を参照し、パケットの中継又は廃棄を判断する。認証要求パケットは、宛先が認証サーバ(2001:200:0:3:2222:00FF:FE11:1111)、送信元ＩＰｖ６インタフェースＩＤがユーザ端末１４００(2222:FFFF:FE00:0001)であるので、＃１のエントリに該当し、中継／廃棄フラグフィールドは、「中継」を

示している。したがって、フィルタリング処理部１３３は、パケットをパケット中継部１１０へ送る。

【０１２５】

パケット中継部１１０は、受け取ったパケットの送信元ＩＰｖ６インタフェースＩＤを抽出し、抽出した送信元ＩＰｖ６インタフェースＩＤを含むエントリがアドレステーブル１６０に存在するか検索する。送信元であるユーザ端末１４００のＩＰｖ６インタフェースＩＤを含むエントリは存在しないため、パケット中継部１１０は、ユーザ端末１４００のＩＰｖ６インタフェースＩＤ、及び、ユーザ端末１４００が接続されているネットワークインタフェース部１２３に対応する識別子「ｃ」を含むエントリを追加する。図２６（ｂ）に、エントリが追加されたアドレステーブル１６０を示す。

【０１２６】

また、パケット中継部１１０は、受け取ったパケットの宛先ＩＰｖ６インタフェースＩＤを抽出し、抽出したＩＰｖ６インタフェースＩＤに基づきアドレステーブル１６０を参照して、中継先のネットワークインタフェース部の識別子を取得する。認証要求パケットは、宛先ＩＰｖ６インタフェースＩＤが(2222:00FF:FE11:1111)であるので、中継先として「ａ」を取得する。パケット中継部１１０は、取得した「ａ」に従って、受け取ったパケットを、ネットワークインタフェース部ａ１２１から認証サーバ２００に送信する（Ｓ４０９）。

【０１２７】

認証サーバ２００は、ユーザ端末１４００から認証要求パケットを受け取ると、ユーザ端末１４００を宛先として、認証パラメータ要求パケットを送信する（Ｓ４１１）。

【０１２８】

ネットワークインタフェース部ａ１２１は、認証サーバ２００から認証パラメータ要求パケットを受け取り、フィルタリング処理部１３１へ送る。フィルタリング処理部１３１のフィルタリングテーブル５２０には何も登録されていないので、フィルタリング処理部１３１は、パケットをパケット中継部１１０へ送る。

【０１２９】

パケット中継部１１０は、上述と同様に、アドレステーブル１６０を参照し、パケットの宛先ＩＰｖ６インタフェースＩＤ(2222:FFFF:FE00:1)に基づき、中継先「ｃ」を取得する。パケット中継部１１０は、パケットをネットワークインタフェース部ｃ１２３に対応したＩＰｓｅｃ処理部１８３へ中継する（Ｓ４１３）。ＩＰｓｅｃ処理部１８３は、ＩＰｓｅｃ制御部１７０からパケットの宛先ＩＰｖ６アドレスに対応する秘密対称鍵を取得し、秘密対称鍵を用いてパケット中継部１１０から受け取ったパケットをＥＳＰ機能により暗号化する。ＩＰｓｅｃ処理部１８３は、暗号化したパケットをネットワークインタフェース部ｃ１２３を介して、ユーザ端末１４００に送信する（Ｓ４１４）。

【０１３０】

ユーザ端末１４００は、認証パラメータ要求パケットを受信すると、ＩＫＥ認証情報、ＩＰｖ６インタフェースＩＤを含むパケットを認証サーバ２００に送信する（Ｓ４１５）。ＩＫＥ認証情報としては、例えば、ｐｒｅ－ｓｈａｒｅｄｋｅｙを用いて所定の計算を行った値を用いることができる。また、ＩＫＥ認証情報は、これ以外にも適宜の値、情報を用いてもよい。ネットワークノード１００のＩＰｓｅｃ処理部１８３、フィルタリング処理部１３３は、ステップＳ４０７、Ｓ４０９と同様の処理により、ユーザ端末１４００からのパケットを認証サーバ２００へ中継する（Ｓ４１７、Ｓ４１９）。

【０１３１】

認証サーバ２００は、ＩＫＥ認証情報、ＩＰｖ６インタフェースＩＤを含むパケットを受け取ると、予め記憶されている情報と比較し、ユーザ認証を行う。ユーザ認証がされると、認証サーバ２００は、ネットワークノード１１００のフィルタ変更指示処理部１４０と通信し、フィルタ変更指示処理部１４０に状態変更指示を送信する（Ｓ４２１）。状態変更指示は、例えば、宛先ＩＰｖ６アドレスとして「任意」、送信元ＩＰｖ６インタフェースＩＤとしてユーザ端末１４００のＩＰｖ６インタフェースＩＤ、及び、パケットの「中継」、エントリの追加を示す情報を含む。

【０１３２】

フィルタ変更指示処理部１４０は、認証サーバ２００からの状態変更指示を受

け取ると、状態変更指示に含まれる送信元ＩＰｖ６インタフェースＩＤに基づき、アドレステーブル１６０を参照する。フィルタ変更指示処理部１４０は、ネットワークインタフェース部の識別子「ｃ」を取得する。フィルタ変更指示処理部１４０は、状態変更指示に従い、取得した識別子「ｃ」に対応するフィルタリング処理部１３３のフィルタリングテーブルの内容を変更する。図２５（ｂ）に、状態変更指示に従いエントリが追加されたフィルタリングテーブルの構成図を示す。これにより、ユーザ認証されたユーザ端末１４００と、サイトＥ内のファイルサーバ３００の通信が可能になる。

【０１３３】

次に、ユーザ端末１４００は、ファイルサーバを宛先として、例えば、ファイルのＲｅａｄ要求を示すパケットを送信する（Ｓ４２３）。ネットワークノード１１００のＩＰｓｅｃ処理部１８３は、上述と同様にして、ユーザ端末１４００からのパケットを受け取り、フィルタリング処理部１３３へ送る（Ｓ４２５）。また、フィルタリング処理部１３３は、上述と同様にして、ＩＰｓｅｃ処理部１８３から受け取ったパケットをパケット中継部１１０へ送る。

【０１３４】

パケット中継部１１０は、宛先ＩＰｖ６インタフェースＩＤに基づきアドレステーブルを参照し、中継先として「ｂ」を取得する。パケット中継部１１０は、ネットワークインタフェース部１２２を介して、パケットをファイルサーバ３００へ送信する（Ｓ４２７）。

【０１３５】

ファイルサーバ３００は、ファイルのＲｅａｄ要求を受け取ると、要求に応じたデータを含むパケットをユーザ端末１４００宛てに送信する（Ｓ４２９）。ネットワークインタフェース部ｂ１２２は、ファイルサーバ３００からパケットを受け取り、フィルタリング処理部１３２へ送る。ステップＳ４１３、Ｓ４１４と同様に、フィルタリング処理部１３２は受け取ったパケットをパケット中継部１１０へ送り、さらに、パケット中継部１１０はＩＰｓｅｃ処理部１３２へ送る（Ｓ４３１）。ＩＰｓｅｃ処理部１３２は、パケットをＥＳＰ機能により秘密対称鍵を用いて暗号化し、ネットワークインタフェース部ｃ１２３を介してパケット

を送信する（Ｓ４３３）。ユーザ端末１４００は、ファイルサーバ３００からのパケットを受信し、ＥＳＰ機能により秘密対称鍵を用いて復号化することにより、データを得ることができる。

【０１３６】

仮に、不正侵入者が同一ＩＰアドレスに成りすましてファイルサーバ３００等にパケットを送信（Ｓ４５１）した場合、不正侵入者の端末はネットワークノード１１００とｐｒｅ－ｓｈａｒｅｄ　ｋｅｙや公開鍵を共有していないため、パケットを受け取ったＩＰｓｅｃ処理部１８３は、ＩＫＥにおける通信相手の認証ができず、当該パケットを廃棄する。

【０１３７】

ＡＤＳＬなどの常時接続ブロードバンドにより企業と家庭（ＳＯＨＯ）や支店を結ぶ場合、通信事業者のインターネットＶＰＮを利用するケースが増えている。従来の認証方式では、ＳＯＨＯは、プロバイダの先にある企業との連携作業によって行なう複雑な認証方式となっている。この複雑な手順を簡素化するのにも、本実施の形態におけるＩＰアドレスフィルタリングを活用することができる。プロバイダは、企業とは関係無く、必要に応じてプロバイダに加入許可のため認証を行う。その後は、ＳＯＨＯと企業がＶＰＮで繋がるが、企業側エッジでは最初に、プロバイダ認証とは独立にユーザ認証を行うことができる。

【０１３８】

以上、広域イーサネット（登録商標）、構内データセンタ、インターネットＶＰＮの事例についてユーザ認証及びパケットフィルタリングについて説明したが、認証及びフィルタリングのパラメータは、それぞれの事例に限定されるものではなく、他の事例及び他のネットワークに対しても用いることができる。

【０１３９】

【発明の効果】

本発明によると、アクセスが許可されていない端末からのアクセス、及び、なりすましによる侵入者からのアクセスを拒否する高セキュリティなネットワークシステムを構築することができる。また、本発明によると、ＩＰｖ６アドレスのインタフェースＩＤ部分を活用してセキュリティ強度の高いユーザ認証及びパケ

ットフィルタリングを行うことができる。特に、ルータを介して通信を行うネットワークシステムにおいて、従来のＩＰｖ４アドレスによるフィルタリングよりも強度の高いセキュリティシステムを提供することができる。また、本発明によると、ユーザ端末の移動に対しても高いセキュリティ強度を有するモビリティの優れたシステムを提供することができる。

【０１４０】

さらに、本発明によると、Ｌ２スイッチにＩＰフィルタリング機能を持たせ、ＭＡＣアドレス及びＩＰアドレス等をパラメータとした多段フィルタリングを行い、セキュリティ強度を高くすることができる。本発明によると、ユーザＩＤ及びパスワードに加えてＩＰｖ６アドレスのインタフェースＩＤ及びＩＫＥのユーザ認証機能を併用することによりユーザ認証の確度を高めることができる。また、本発明によると、広域イーサネット（登録商標）、構内データセンタ、インターネットＶＰＮ等のネットワークにおける高セキュリティなネットワークシステムを提供することができる。

【図面の簡単な説明】

【図１】

ネットワーク認証システムの基本構成図。

【図２】

ＩＰｖ６認証ノードの構成図。

【図３】

フィルタリング処理部の構成図。

【図４】

認証サーバの構成図。

【図５】

認証処理部を内蔵した認証ノードの構成図。

【図６】

認証処理部の構成図。

【図７】

ＩＰｖ６アドレスのアドレスフォーマット。

【図８】

フィルタリングテーブルの構成例（１）を示す図。

【図９】

フィルタリングテーブルの構成例（２）を示す図。

【図１０】

アドレステーブルの構成例（１）を示す図。

【図１１】

パケット処理部の処理の詳細説明図。

【図１２】

フィルタリング処理部の他の構成図。

【図１３】

ＭＡＣアドレスフィルタリングテーブル及びＩＰｖ６アドレスフィルタリングテーブルの構成図。

【図１４】

広域イーサネット（登録商標）網におけるネットワーク認証システムの構成図。

【図１５】

ユーザ端末のエントリが追加されたアドレステーブルの構成図。

【図１６】

広域イーサネット（登録商標）網におけるネットワーク認証システムのシーケンス図。

【図１７】

状態変更指示に従い変更されたフィルタリングテーブルの構成図。

【図１８】

構内データセンタにネットワークノードを適用したネットワーク認証システムの構成図。

【図１９】

フィルタリングテーブルの構成例（３）を示す図。

【図２０】

アドレステーブルの構成例（２）を示す図。

【図２１】

構内データセンタにネットワークノードを適用したネットワーク認証システムのシーケンス図。

【図２２】

インターネットＶＰＮにおけるネットワーク認証システムの構成図。

【図２３】

ＩＰｓｅｃ通信が可能なネットワークノードの構成図。

【図２４】

キーテーブルの構成例を示す図。

【図２５】

フィルタリングテーブルの構成例（４）を示す図。

【図２６】

アドレステーブルの構成例（３）を示す図。

【図２７】

インターネットＶＰＮにおけるネットワーク認証システムのシーケンス図。

【図２８】

マルチレイヤスイッチによるフィルタリング処理の概略図。

【符号の説明】

１００　認証ノード（ネットワークノード）

１１０　パケット中継部

１２１～１２５　ネットワークインタフェース部ａ～ｅ

１３１～１３５　フィルタリング処理部

１４０　フィルタ変更指示処理部

１５０　ＩＰｖ６処理部

１６０　アドレステーブル

２００　認証サーバ

２１０　認証受付処理部

２２０　認証部

２５０　認証処理部

２６０　認証受付処理部

２７０　認証部

３００　情報サーバ

４００　情報端末（ユーザ端末）

５１０　パケット処理部

５２０　フィルタリングテーブル

５３０　ＭＡＣアドレス処理部

５４０　ＩＰｖ６アドレス処理部

５５０　ＭＡＣアドレスフィルタリングテーブル

５６０　ＩＰｖ６アドレスフィルタリングテーブル

６００　広域イーサネット（登録商標）網

６１０　回線終端装置

７００　構内データセンタ

７１０　ルータ

７２０　ＬＡＮスイッチ

７３０、５０　情報コンセント

８００　インターネット

８１０、８２０　回線終端装置

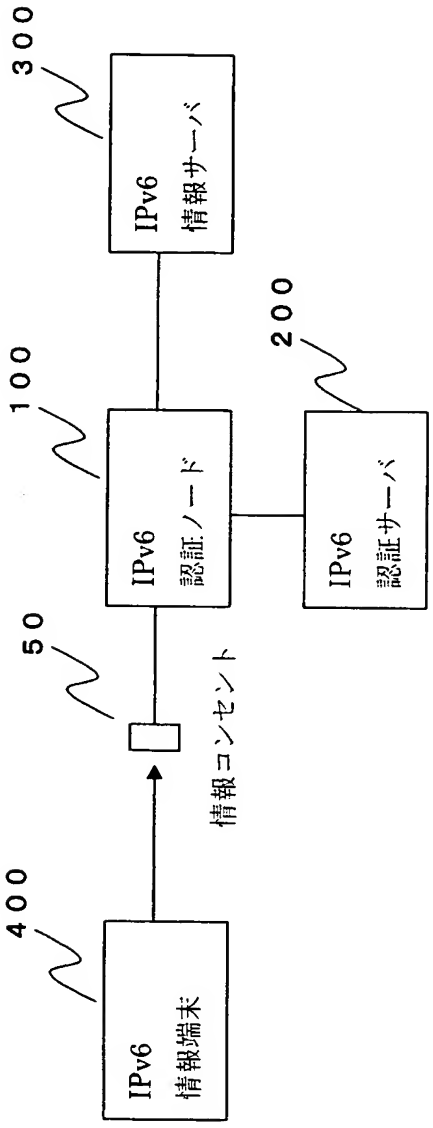
１１００　ネットワークノード

１４００　ＩＰｓｅｃユーザ端末

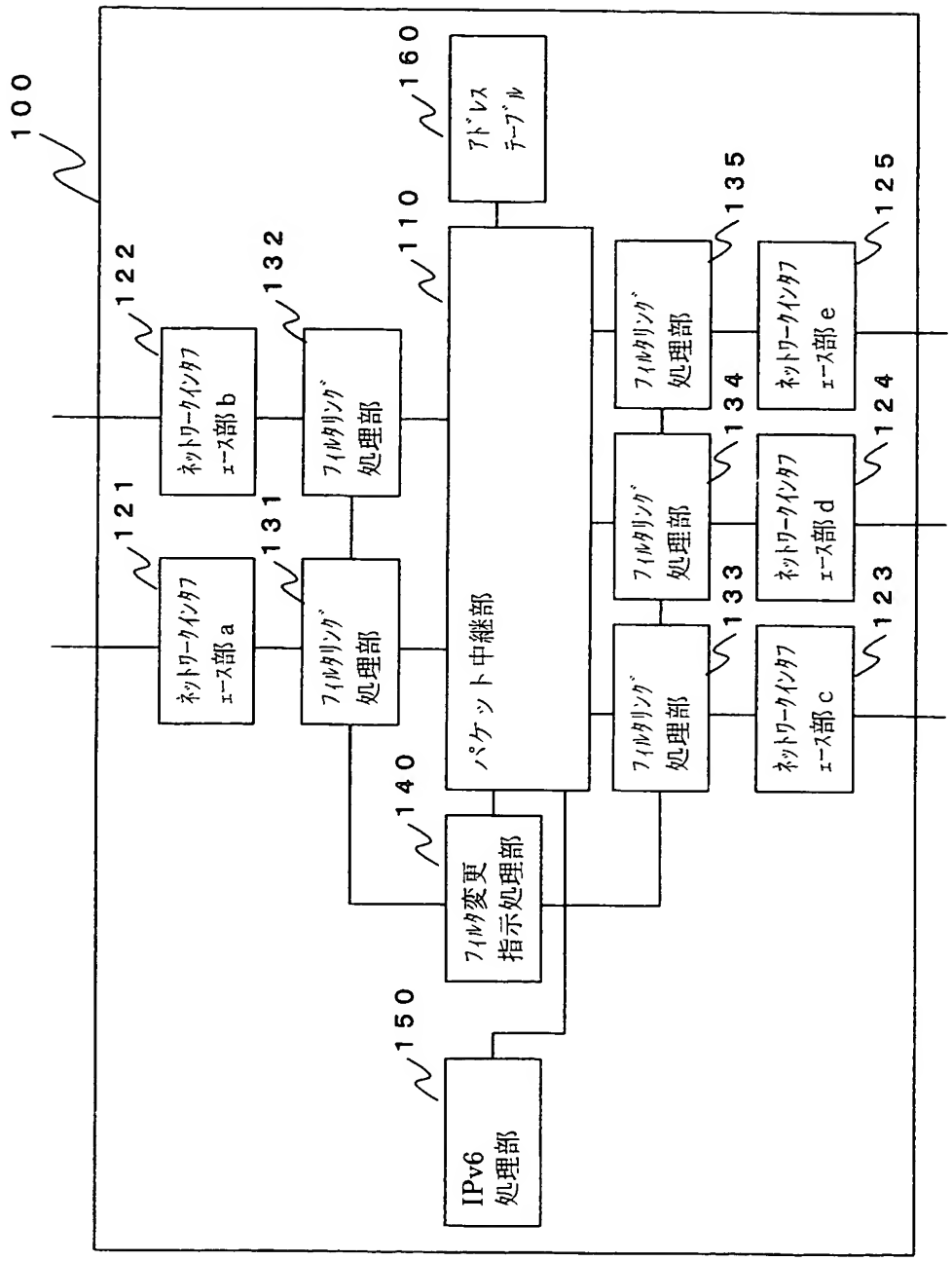
２１００　認証処理部内蔵ネットワークノード

【書類名】図面

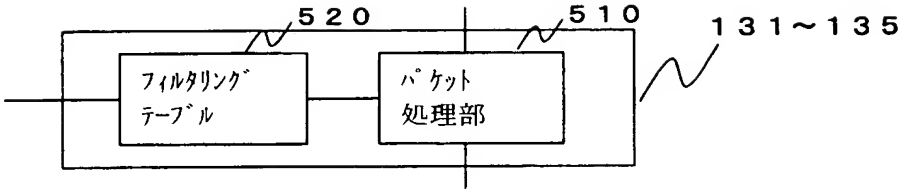
【図１】


300
IPv6
情報サーバ
200
100
IPv6
認証ノード
IPv6
認証サーバ
50
情報コンセント
400
IPv6
情報端末

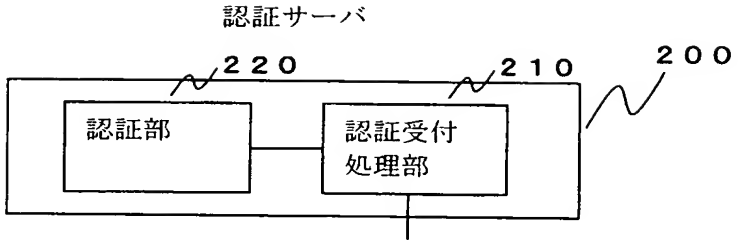
【図２】


100
160
アドレス テーブル
110
パケット中継部
122
ネットワークインタフェース部 b
132
フィルタリング処理部
121
ネットワークインタフェース部 a
131
フィルタリング処理部
135
フィルタリング処理部
125
ネットワークインタフェース部 e
134
フィルタリング処理部
124
ネットワークインタフェース部 d
133
フィルタリング処理部
123
ネットワークインタフェース部 c
140
フィルタ変更指示処理部
150
IPv6 処理部

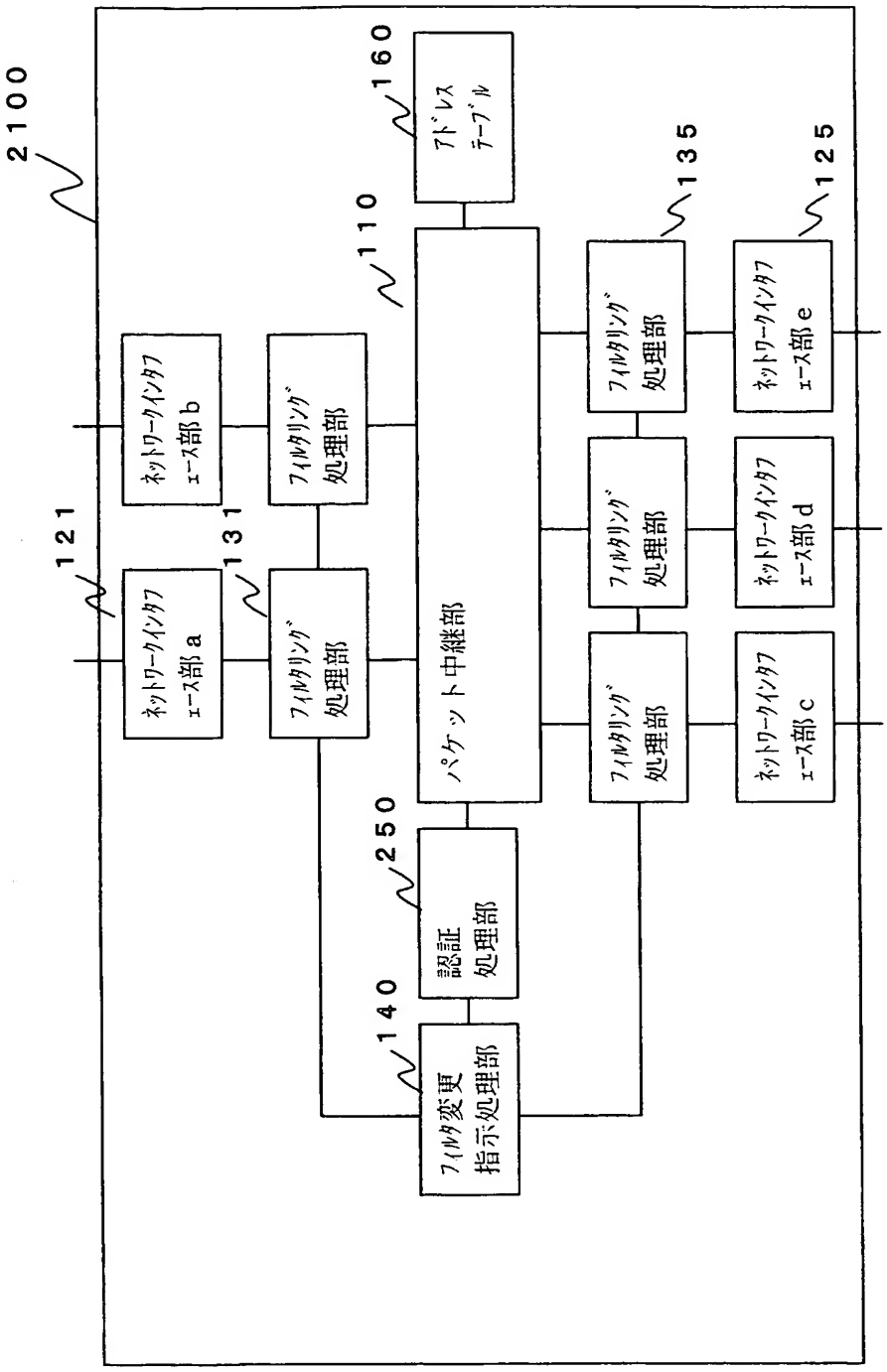
【図３】



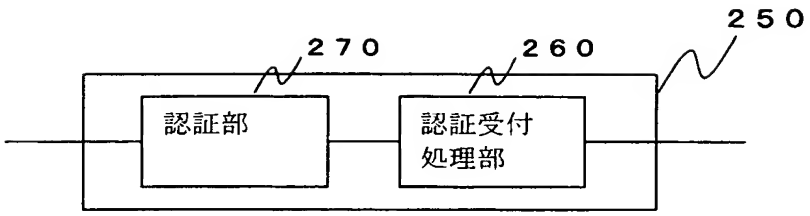
【図４】



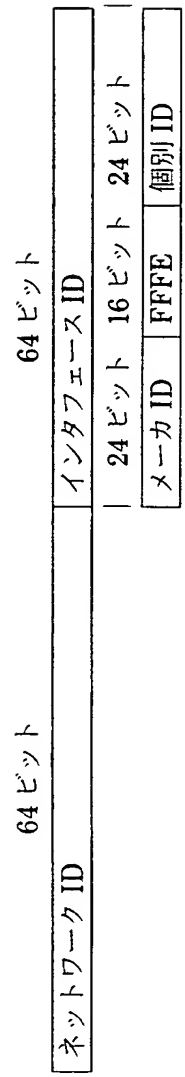
【図５】


2100
121
131
110
160
135
125
250
140
ネットワークインタフェース部a
ネットワークインタフェース部b
ネットワークインタフェース部c
ネットワークインタフェース部d
ネットワークインタフェース部e
フィルタリング処理部
フィルタリング処理部
フィルタリング処理部
フィルタリング処理部
フィルタリング処理部
パケット中継部
アドレステーブル
認証処理部
フィルタ変更指示処理部

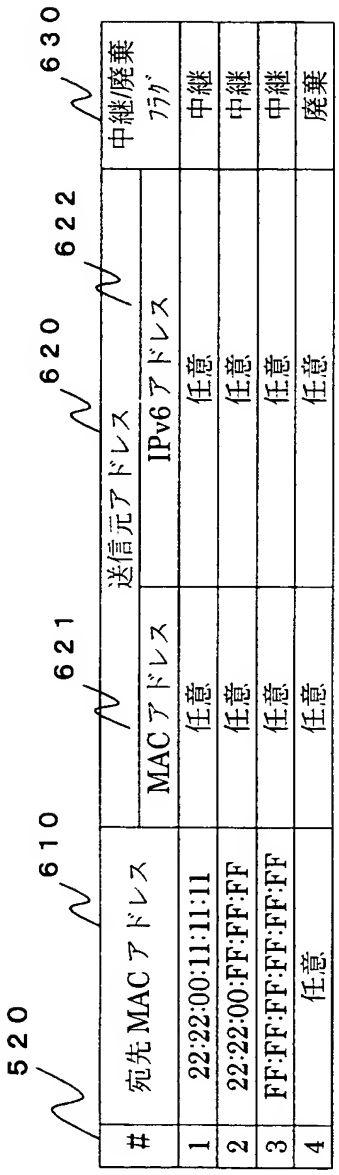
【図６】



【図７】

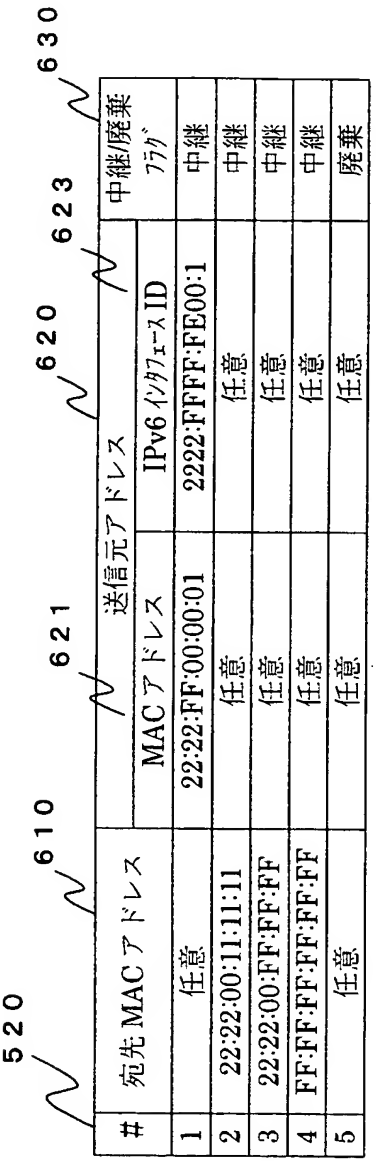

64 ビット
ネットワーク ID
64 ビット
インタフェース ID
24 ビット
16 ビット
24 ビット
メーカ ID
FFFE
個別 ID

【図８】



#	宛先MACアドレス	送信元アドレス		中継/廃棄フラグ
		MACアドレス	IPv6アドレス	
1	22:22:00:11:11:11	任意	任意	中継
2	22:22:00:FF:FF:FF	任意	任意	中継
3	FF:FF:FF:FF:FF:FF	任意	任意	中継
4	任意	任意	任意	廃棄

【図９】



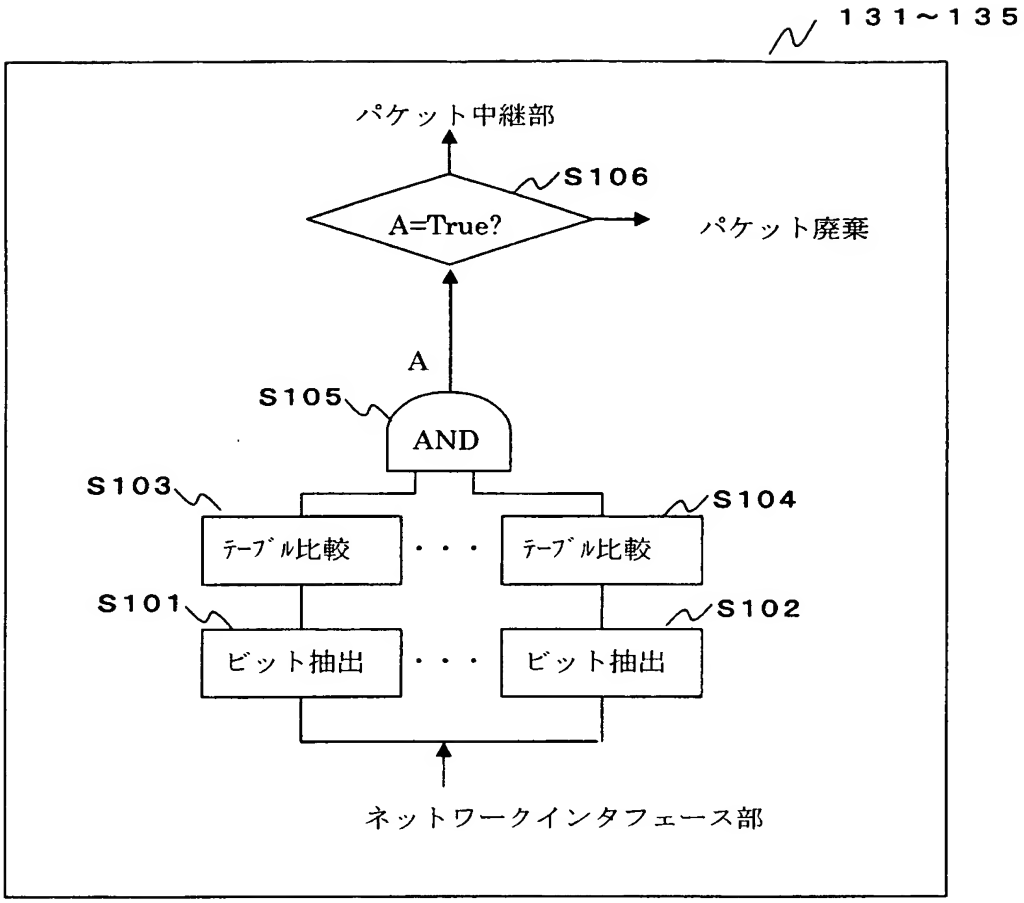
#	宛先 MAC アドレス	送信元アドレス		中継/廃棄フラグ
		MAC アドレス	IPv6 インタフェース ID	
1	任意	22:22:FF:00:00:01	2222:FFFF:FE00:1	中継
2	22:22:00:11:11:11	任意	任意	中継
3	22:22:00:FF:FF:FF	任意	任意	中継
4	FF:FF:FF:FF:FF:FF	任意	任意	中継
5	任意	任意	任意	廃棄

【図１０】

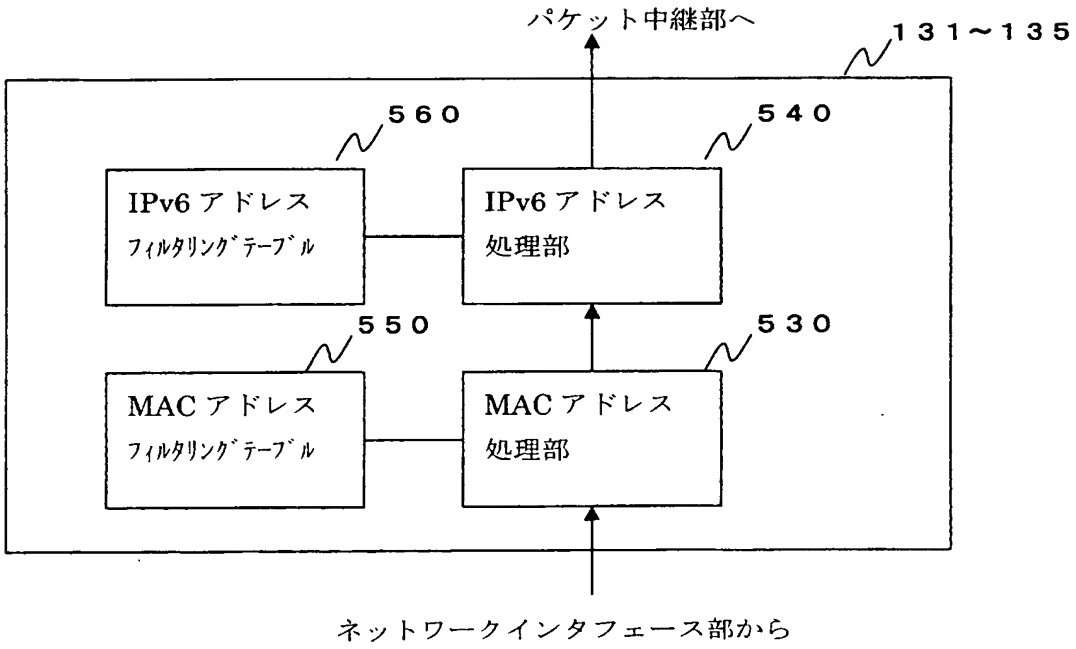
MACアドレス (161)	ネットワークインタフェース部 (162)
22:22:00:11:11:11	c
22:22:FF:22:22:22	d
22:22:00:FF:FF:FF	x
FF:FF:FF:FF:FF:FF	x

(160)

【図１１】


１３１～１３５
パケット中継部
S106
A=True?
パケット廃棄
A
S105
AND
S103
S104
ﾃｰﾌﾞﾙ比較
・・・
ﾃｰﾌﾞﾙ比較
S101
S102
ビット抽出
・・・
ビット抽出
ネットワークインタフェース部

【図１２】


パケット中継部へ
１３１～１３５
５６０
５４０
IPv6 アドレス
ﾌｨﾙﾀﾘﾝｸﾞﾃｰﾌﾞﾙ
IPv6 アドレス
処理部
５５０
５３０
MAC アドレス
ﾌｨﾙﾀﾘﾝｸﾞﾃｰﾌﾞﾙ
MAC アドレス
処理部
ネットワークインタフェース部から

【図１３】

550　610　621　630

#	宛先 MAC アドレス	送信元 MAC アドレス	中継/廃棄 ﾌﾗｸﾞ
1	22:22:00:11:11:11	任意	中継
2	22:22:00:FF:FF:FF	任意	中継
3	FF:FF:FF:FF:FF:FF	任意	中継
4	任意	任意	廃棄

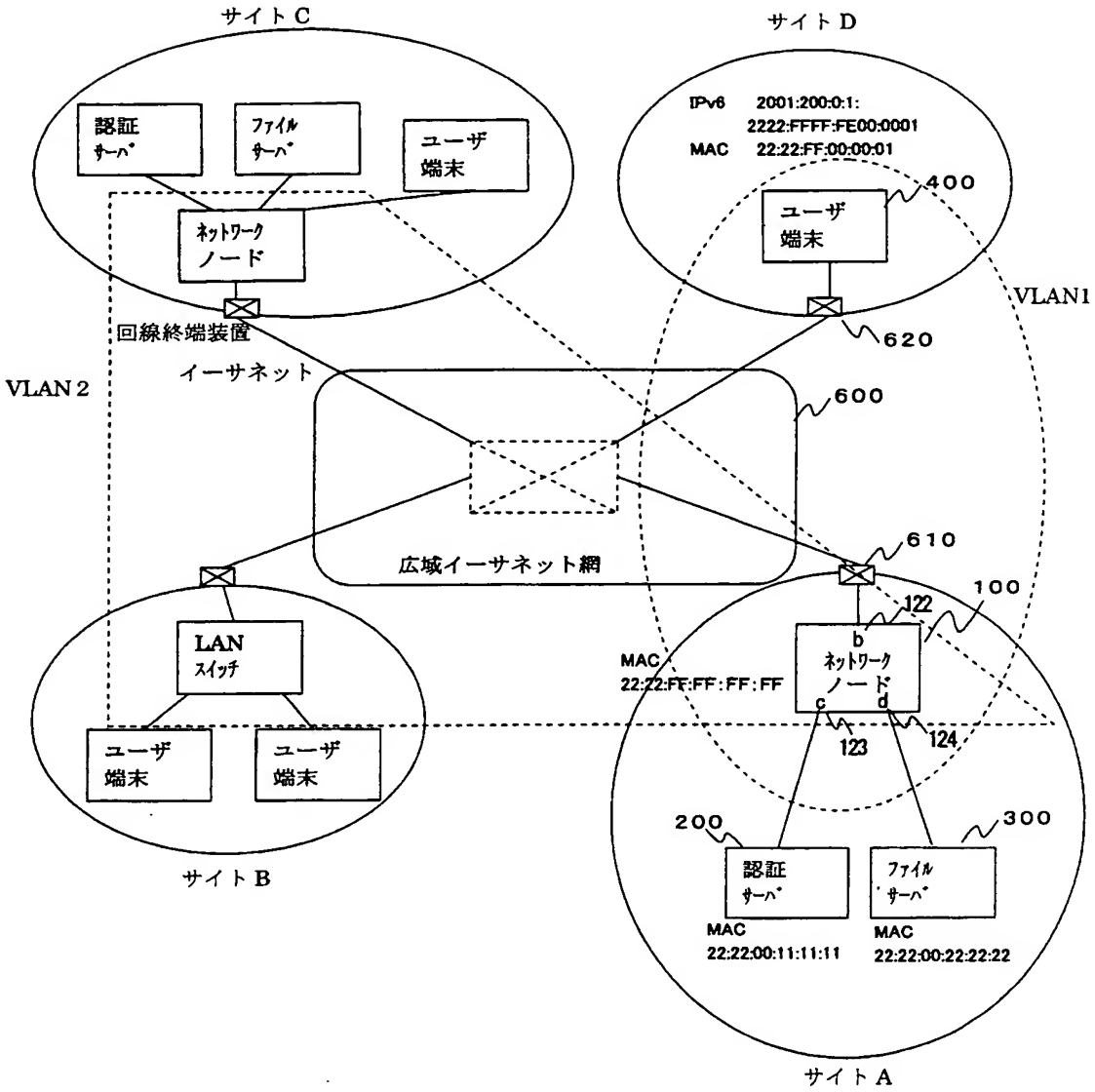
（ａ）

560　610　622　630

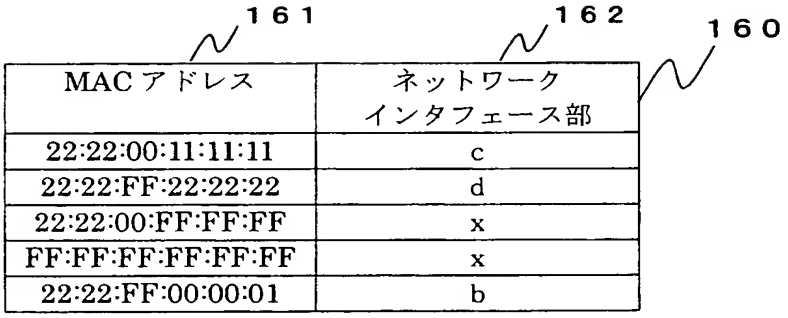
#	宛先 MAC アドレス	送信元 IPv6 アドレス	中継/廃棄 ﾌﾗｸﾞ
1	22:22:00:11:11:11	任意	中継
2	22:22:00:FF:FF:FF	任意	中継
3	FF:FF:FF:FF:FF:FF	任意	中継
4	任意	任意	廃棄

（ｂ）

【図１４】

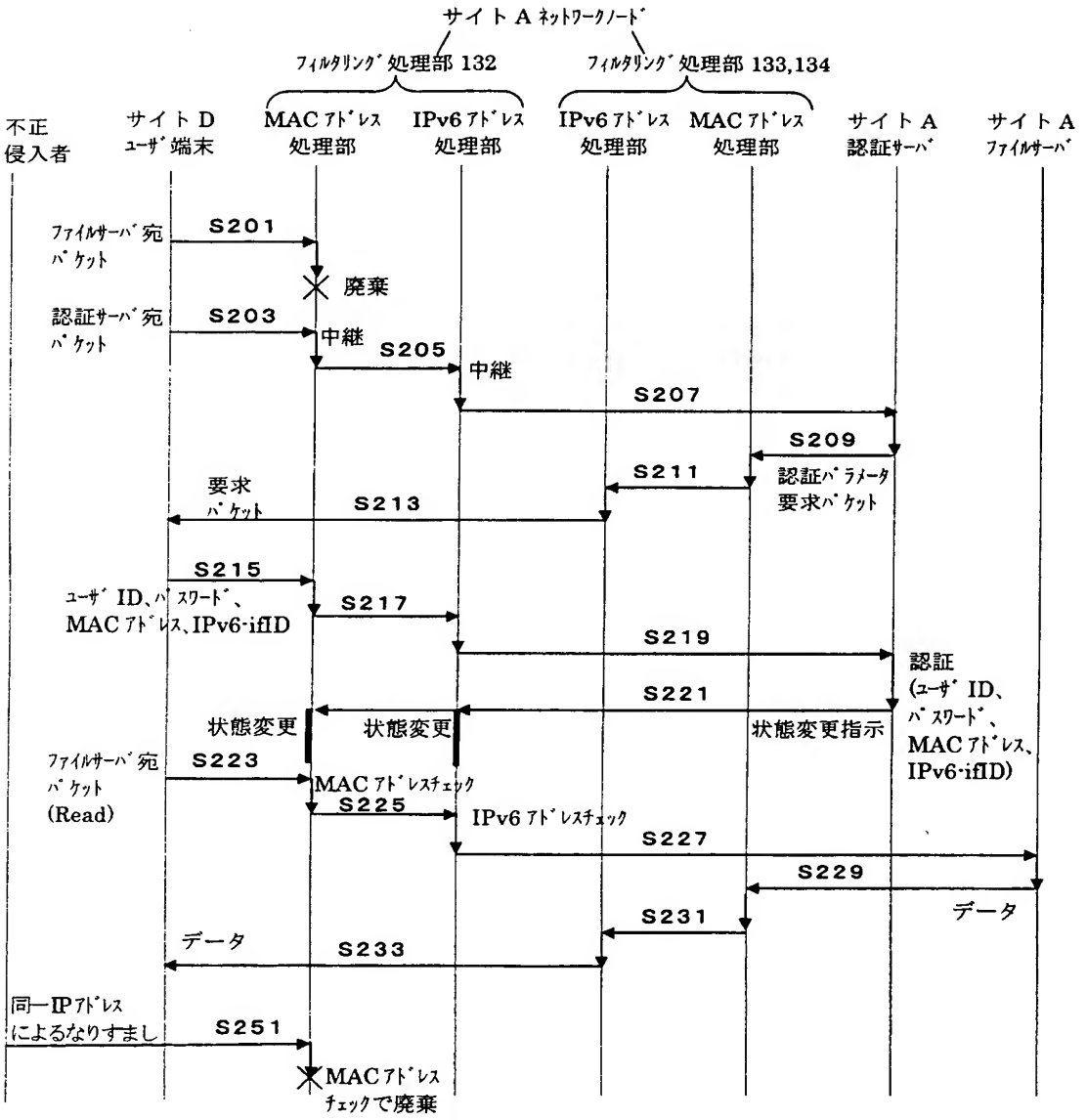

サイトC
サイトD
認証
ｻｰﾊﾞ
ファイル
ｻｰﾊﾞ
ユーザ
端末
ネットワーク
ノード
IPv6　2001:200:0:1:
2222:FFFF:FE00:0001
MAC　22:22:FF:00:00:01
400
ユーザ
端末
VLAN1
回線終端装置
620
イーサネット
VLAN 2
600
広域イーサネット網
610
100
122
b
ネットワーク
ノード
c
d
123
124
MAC
22:22:FF:FF:FF:FF
LAN
ｽｲｯﾁ
ユーザ
端末
ユーザ
端末
200
300
認証
ｻｰﾊﾞ
ファイル
ｻｰﾊﾞ
MAC
22:22:00:11:11:11
MAC
22:22:00:22:22:22
サイトB
サイトA

【図１５】

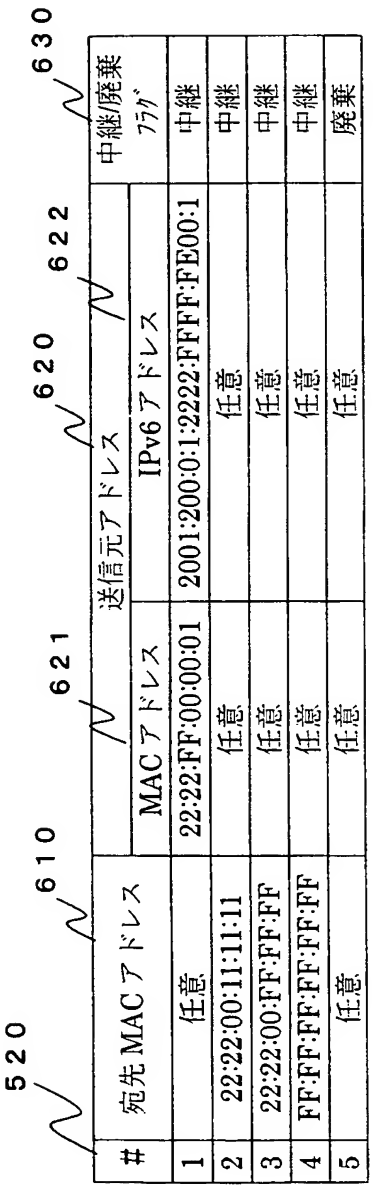


MACアドレス	ネットワーク インタフェース部
22:22:00:11:11:11	c
22:22:FF:22:22:22	d
22:22:00:FF:FF:FF	x
FF:FF:FF:FF:FF:FF	x
22:22:FF:00:00:01	b

【図１６】

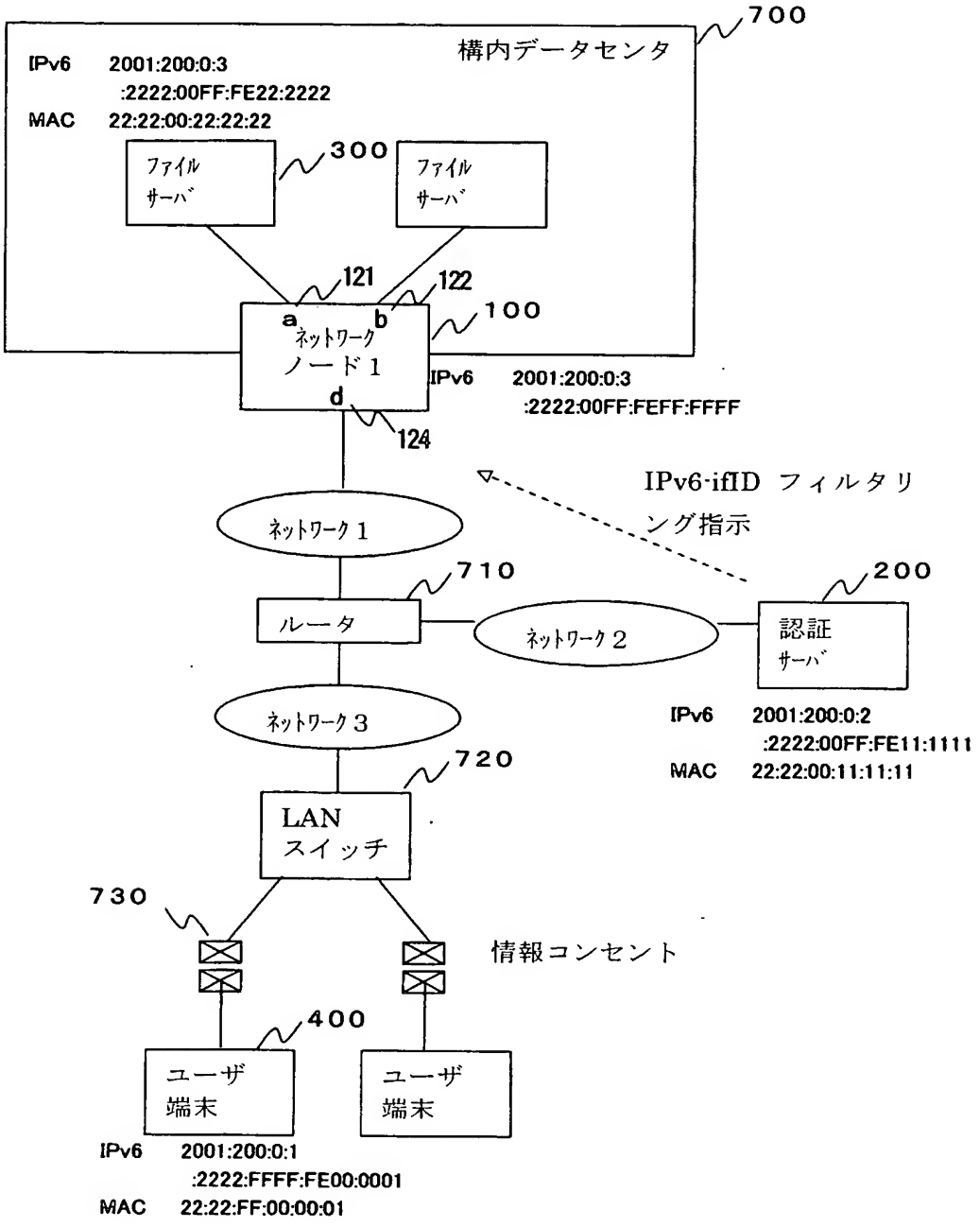

サイトＡネットワークノード
フィルタリング処理部 132
フィルタリング処理部 133,134
不正侵入者
サイトＤ ユーザ端末
MACアドレス処理部
IPv6アドレス処理部
IPv6アドレス処理部
MACアドレス処理部
サイトＡ 認証サーバ
サイトＡ ファイルサーバ
ファイルサーバ宛パケット
S201
廃棄
認証サーバ宛パケット
S203
中継
S205
中継
S207
S209
認証パラメータ要求パケット
S211
要求パケット
S213
S215
ユーザID、パスワード、MACアドレス、IPv6-ifID
S217
S219
認証（ユーザID、パスワード、MACアドレス、IPv6-ifID）
S221
状態変更
状態変更
状態変更指示
ファイルサーバ宛パケット（Read）
S223
MACアドレスチェック
S225
IPv6アドレスチェック
S227
S229
データ
S231
データ
S233
同一IPアドレスによるなりすまし
S251
MACアドレスチェックで廃棄

【図１７】

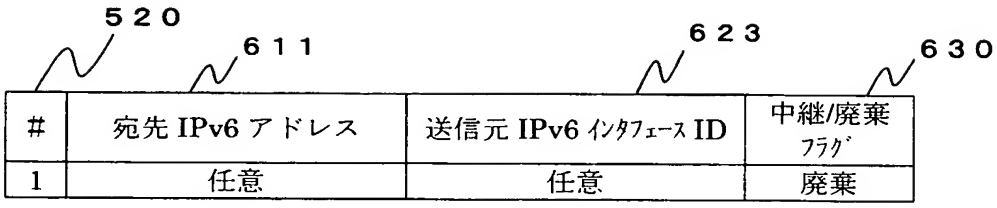


#	宛先MACアドレス	送信元アドレス		中継/廃棄フラグ
		MACアドレス	IPv6アドレス	
1	任意	22:22:FF:00:00:01	2001:200:0:1:2222:FFFF:FE00:1	中継
2	22:22:00:11:11:11	任意	任意	中継
3	22:22:00:FF:FF:FF	任意	任意	中継
4	FF:FF:FF:FF:FF:FF	任意	任意	中継
5	任意	任意	任意	廃棄

【図１８】

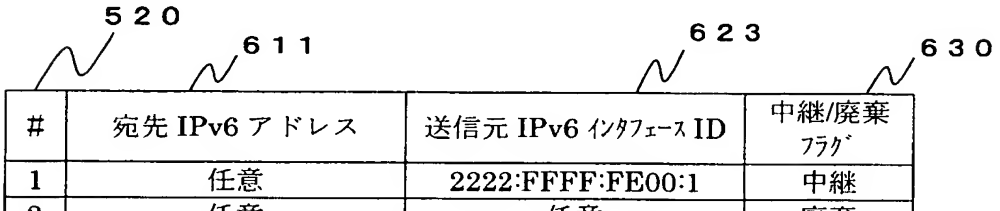

700
構内データセンタ
IPv6　2001:200:0:3
:2222:00FF:FE22:2222
MAC　22:22:00:22:22:22
ファイル
サーバ
300
ファイル
サーバ
121
122
a
b
ネットワーク
ノード１
100
IPv6　2001:200:0:3
:2222:00FF:FEFF:FFFF
d
124
IPv6-ifID フィルタリング指示
ネットワーク１
710
ルータ
ネットワーク２
200
認証
サーバ
IPv6　2001:200:0:2
:2222:00FF:FE11:1111
MAC　22:22:00:11:11:11
ネットワーク３
720
LAN
スイッチ
730
情報コンセント
400
ユーザ
端末
ユーザ
端末
IPv6　2001:200:0:1
:2222:FFFF:FE00:0001
MAC　22:22:FF:00:00:01

【図１９】



#	宛先 IPv6 アドレス	送信元 IPv6 ｲﾝﾀﾌｪｰｽ ID	中継/廃棄 ﾌﾗｸﾞ
1	任意	任意	廃棄

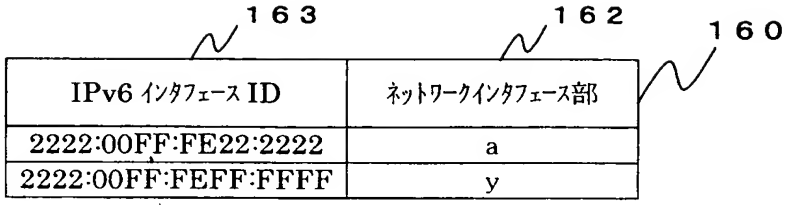
（ａ）



#	宛先 IPv6 アドレス	送信元 IPv6 ｲﾝﾀﾌｪｰｽ ID	中継/廃棄 ﾌﾗｸﾞ
1	任意	2222:FFFF:FE00:1	中継
2	任意	任意	廃棄

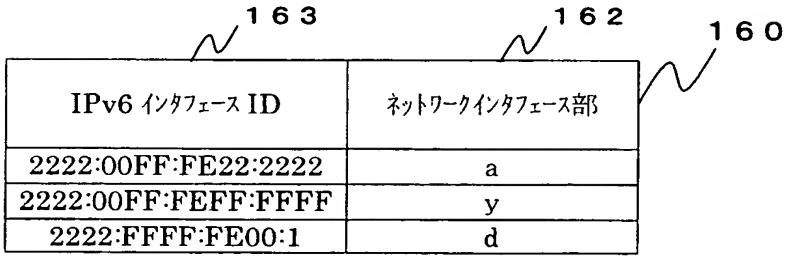
（ｂ）

【図２０】



IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE22:2222	a
2222:00FF:FEFF:FFFF	y

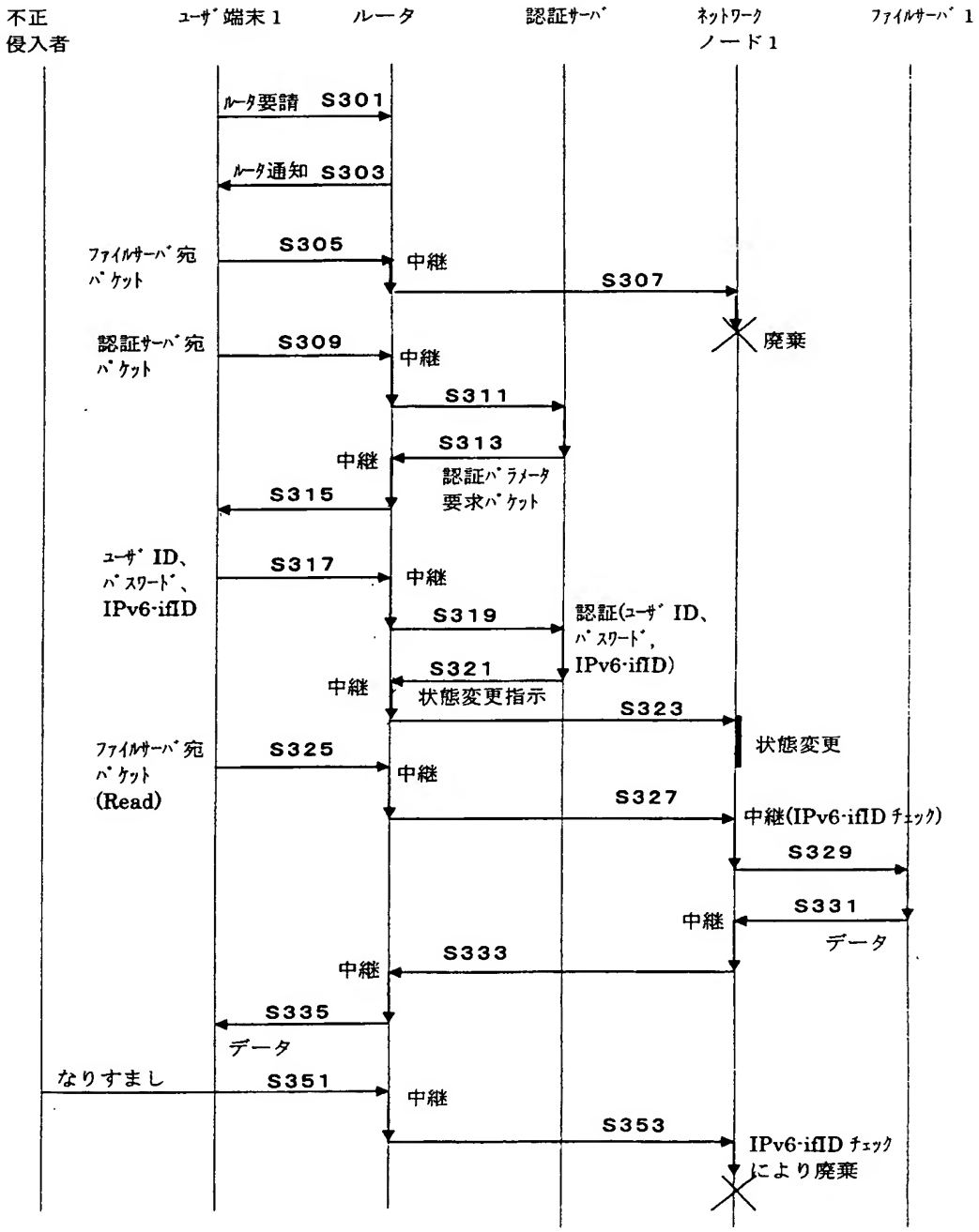
（ａ）



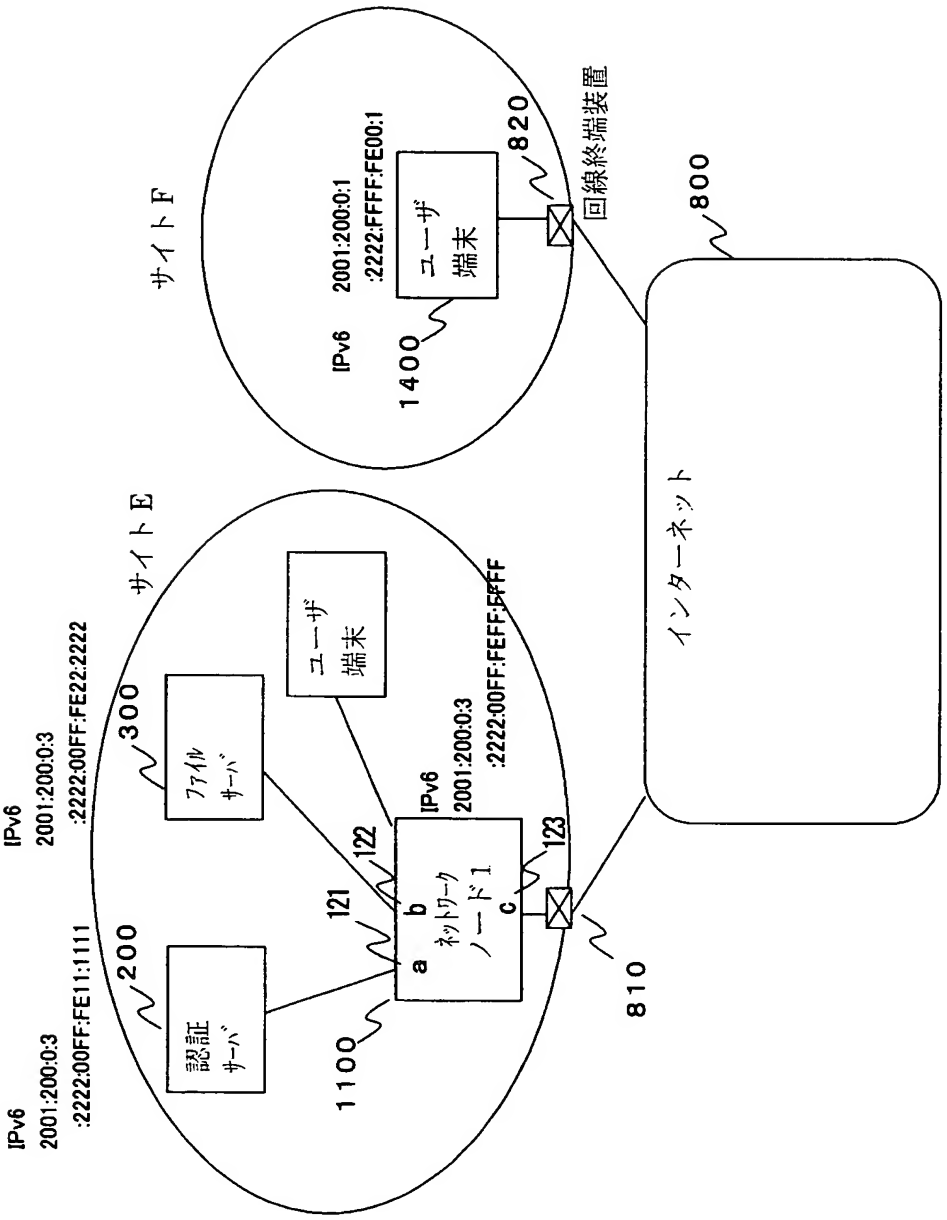
IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE22:2222	a
2222:00FF:FEFF:FFFF	y
2222:FFFF:FE00:1	d

（ｂ）

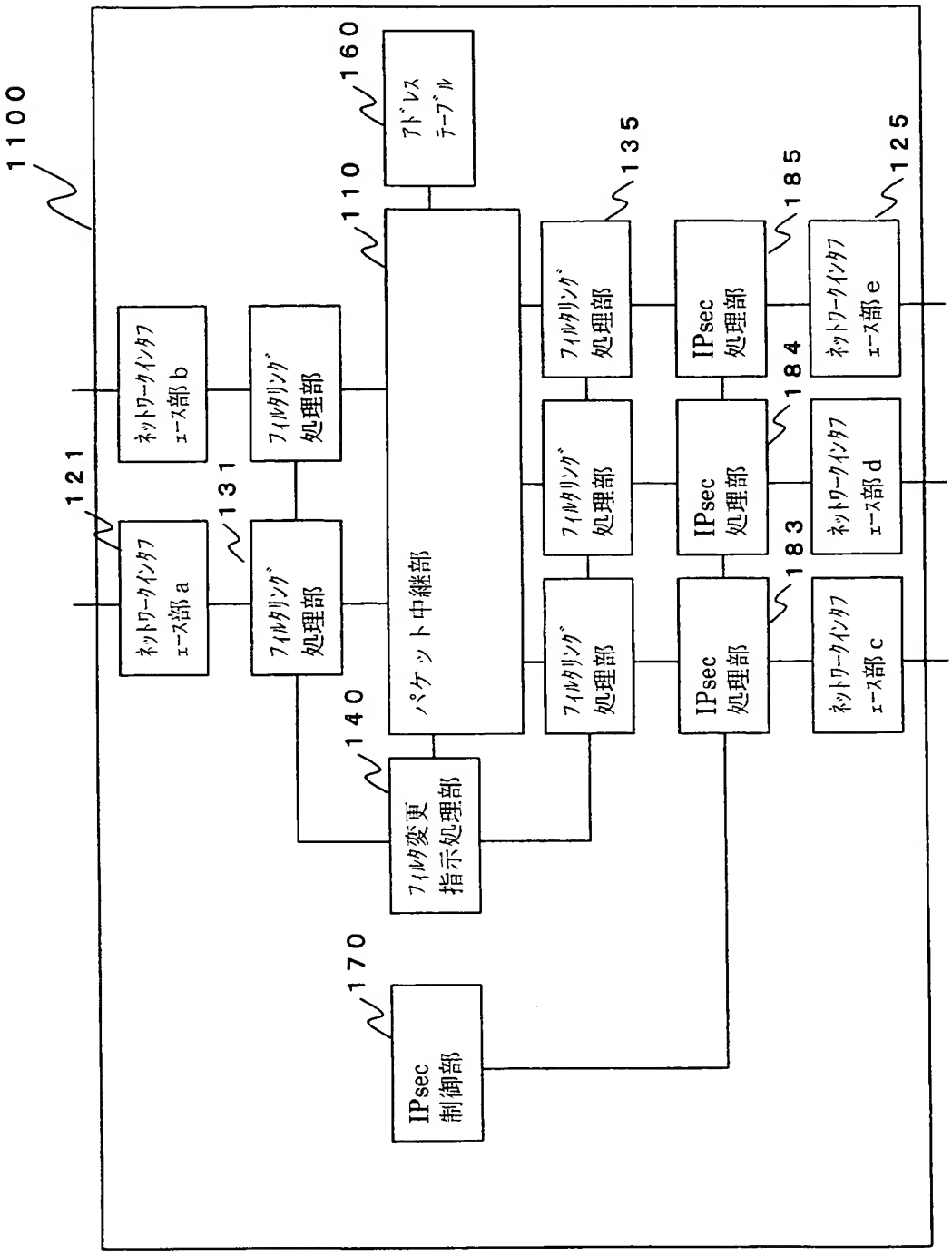
【図２１】


不正
侵入者
ユーザ端末１
ルータ
認証サーバ
ネットワーク
ノード１
ファイルサーバ１
ルータ要請 S301
ルータ通知 S303
S305
ファイルサーバ宛
パケット
中継
S307
廃棄
認証サーバ宛
パケット
S309
中継
S311
S313
中継
認証パラメータ
要求パケット
S315
ユーザ ID、
パスワード、
IPv6-ifID
S317
中継
S319
認証(ユーザ ID、
パスワード、
IPv6-ifID)
S321
中継
状態変更指示
S323
状態変更
ファイルサーバ宛
パケット
(Read)
S325
中継
S327
中継(IPv6-ifID チェック)
S329
S331
中継
データ
S333
中継
S335
データ
なりすまし
S351
中継
S353
IPv6-ifID チェック
により廃棄

【図２２】


サイトF
IPv6
2001:200:0:1
:2222:FFFF:FE00:1
ユーザ
端末
1400
820
回線終端装置
800
インターネット
サイトE
IPv6
2001:200:0:3
:2222:00FF:FE22:2222
300
ファイル
サーバ
ユーザ
端末
IPv6
2001:200:0:3
:2222:00FF:FEFF:FFFF
121
122
123
a
b
ネットワーク
ノード1
c
IPv6
2001:200:0:3
:2222:00FF:FE11:1111
200
認証
サーバ
1100
810

【図２３】


1100
160
アドレス
テーブル
110
パケット中継部
121
ネットワークインタフェース部 a
131
フィルタリング処理部
140
フィルタ変更指示処理部
170
IPsec 制御部
ネットワークインタフェース部 b
フィルタリング処理部
フィルタリング処理部
フィルタリング処理部
135
IPsec 処理部
IPsec 処理部
IPsec 処理部
183
184
185
ネットワークインタフェース部 c
ネットワークインタフェース部 d
ネットワークインタフェース部 e
125

【図２４】

ユーザ端末 IPv6 アドレス	Pre-shared　key	秘密対称鍵
2001:200:0:1 2222:FFFF:FE00:1	Pre-key a	Secret　α
・ ・	Pre-key b	Secret　β
・ ・	・ ・	・ ・

【図２５】

520

#	611 宛先 IPv6 アドレス	623 送信元 IPv6 ｲﾝﾀﾌｪｰｽ ID	630 中継/廃棄 ﾌﾗｸﾞ
1	2001:200:0:3 :2222:00FF:FE11:1111	任意	中継
2	任意	任意	廃棄

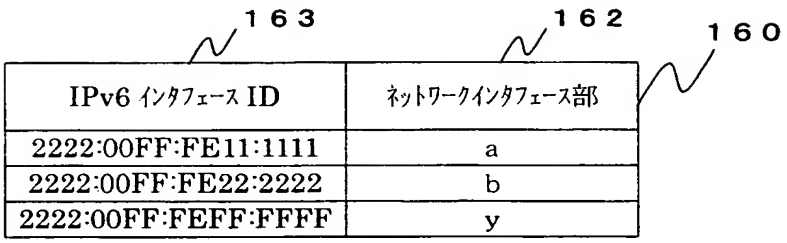
（ａ）

520

#	611 宛先 IPv6 アドレス	623 送信元 IPv6 ｲﾝﾀﾌｪｰｽ ID	630 中継/廃棄 ﾌﾗｸﾞ
1	任意	2222:FFFF:FE00:1	中継
2	2001:200:0:3 :2222:00FF:FE11:1111	任意	中継
3	任意	任意	廃棄

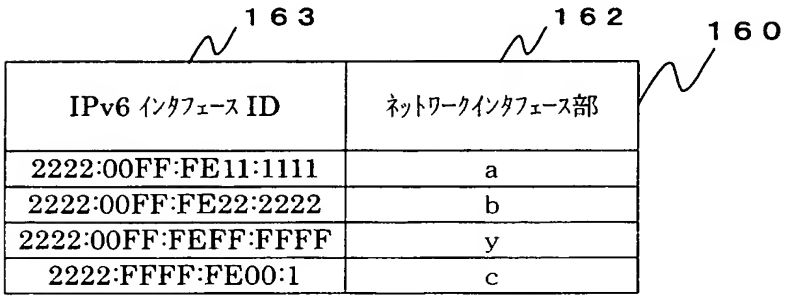
（ｂ）

【図２６】



IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE11:1111	a
2222:00FF:FE22:2222	b
2222:00FF:FEFF:FFFF	y

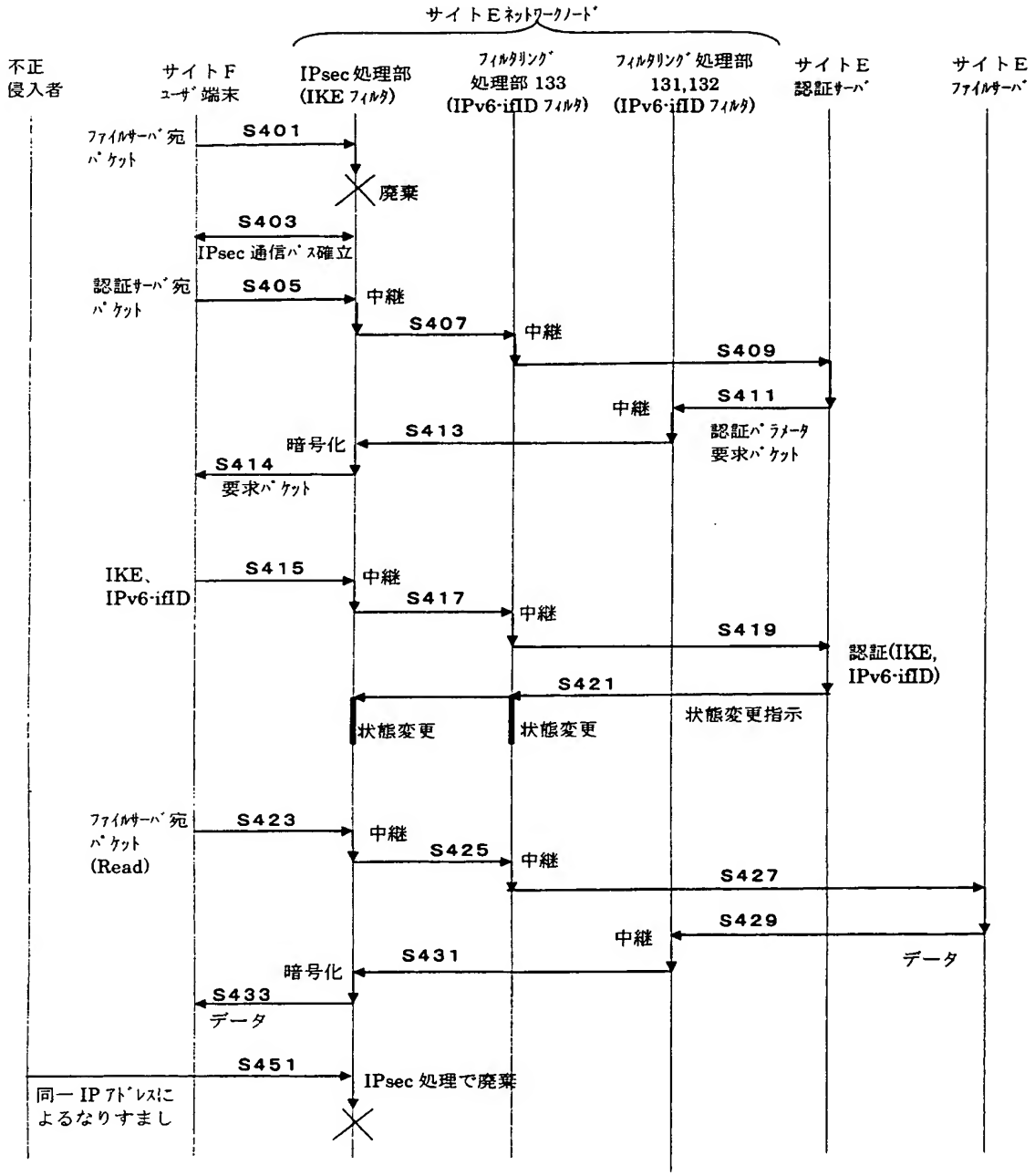
（ａ）



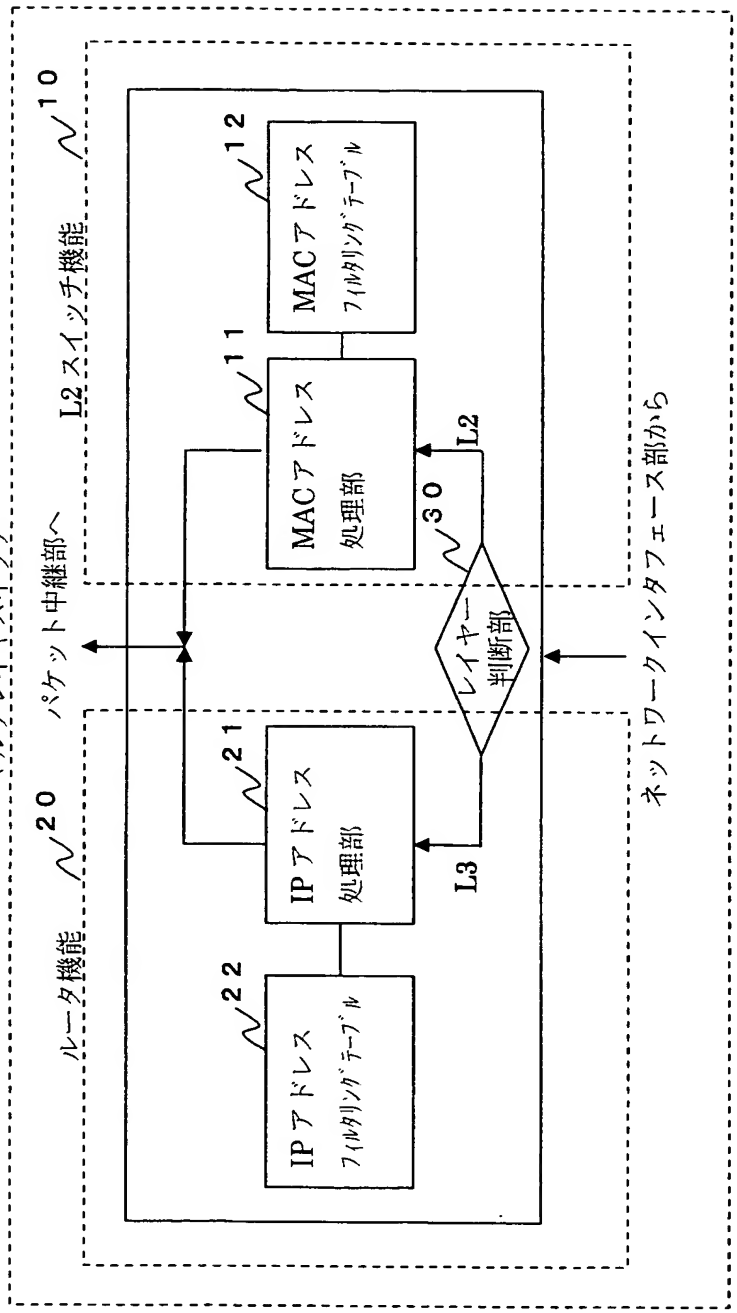
IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE11:1111	a
2222:00FF:FE22:2222	b
2222:00FF:FEFF:FFFF	y
2222:FFFF:FE00:1	c

（ｂ）

【図２７】


サイトEネットワークノード
不正侵入者
サイトF ユーザ端末
IPsec処理部 (IKEフィルタ)
フィルタリング処理部 133 (IPv6-ifIDフィルタ)
フィルタリング処理部 131,132 (IPv6-ifIDフィルタ)
サイトE 認証サーバ
サイトE ファイルサーバ
ファイルサーバ宛パケット
S401
廃棄
S403
IPsec 通信パス確立
認証サーバ宛パケット
S405
中継
S407
中継
S409
S411
中継
認証パラメータ要求パケット
S413
暗号化
S414
要求パケット
IKE、IPv6-ifID
S415
中継
S417
中継
S419
認証(IKE, IPv6-ifID)
S421
状態変更
状態変更
状態変更指示
ファイルサーバ宛パケット (Read)
S423
中継
S425
中継
S427
S429
中継
データ
S431
暗号化
S433
データ
S451
同一IPアドレスによるなりすまし
IPsec処理で廃棄

【図２８】


マルチレイヤスイッチ
10
L2スイッチ機能
パケット中継部へ
12
MACアドレス
フィルタリングテーブル
11
MACアドレス
処理部
L2
30
レイヤー
判断部
ネットワークインタフェース部から
20
ルータ機能
21
IPアドレス
処理部
L3
22
IPアドレス
フィルタリングテーブル

【書類名】　要約書

【要約】

【課題】　アクセスが許可されていない端末、及び、なりすましによる侵入者からのアクセスを拒否するネットワークシステムを提供する。

【解決手段】　認証ノード１００のフィルタリング処理部１３１～１３５は、ネットワークインタフェース部を介して受け取ったパケットが、アクセスを許可された端末からのパケットか、ＭＡＣアドレス、ＩＰｖ６アドレスに基づきフィルタリングテーブルを参照して判断し、パケットを中継又は廃棄する。パケット中継部１１０は、アドレステーブル１６０を参照し、適宜のネットワークインタフェース部を介してフィルタリング処理部を通過したパケットを宛先アドレスへ中継する。フィルタ変更指示処理部１４０は、アクセスが許可されたユーザ端末からのパケットを中継させるための状態変更指示を受信し、フィルタリング処理部のフィルタリングテーブルを変更する。

【選択図】　図２

特願２００３－０７５８６５

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所